

Footprinting and Reconnaissance

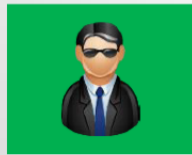
Module 02



Footprinting and Reconnaissance

Module 02

Engineered by **Hackers**. Presented by Professionals.



Ethical Hacking and Countermeasures v8

Module 02: Footprinting and Reconnaissance

Exam 312-50



Security News

Facebook a 'treasure trove' of Personally Identifiable Information

Source: <http://www.scmagazineuk.com>

Facebook contains a "treasure trove" of **personally identifiable information** that hackers manage to get their hands on.

A report by Imperva revealed that users' "**general personal information**" can often include a date of birth, home address and sometimes mother's maiden name, allowing hackers to access this and other websites and applications and create targeted **spearphishing** campaigns.

It detailed a concept I call "friend-mapping", where an attacker can get further knowledge of a user's circle of friends; having accessed their account and posing as a trusted friend, they can cause mayhem. This can include requesting the transfer of funds and extortion.

Asked why Facebook is so important to hackers, **Imperva senior security** strategist Noa Bar-Yosef said: "People also add work friends on Facebook so a team leader can be identified and this can lead to corporate data being accessed, project work being discussed openly, while geo-location data can be detailed for military intelligence."

“Hacktivism made up 58 per cent of attacks in the **Verizon Data Breach Intelligence Report**, and they are going after information on Facebook that can be used to humiliate a person. All types of attackers have their own techniques.”

On how attackers get a password in the first place, Imperva claimed that different **keyloggers** are used, while phishing kits that create a **fake Facebook login page** have been seen, and a more primitive method is a brute force attack, where the attacker repeatedly attempts to guess the user's password.

In more extreme cases, a **Facebook administrator's** rights can be accessed. Although it said that this requires more effort on the hacker side and is not as prevalent, it is the “**holy grail**” of attacks as it provides the hacker with data on all users.

On protection, Bar-Yosef said the roll-out of SSL across the whole website, rather than just at the login page, was effective, but users still needed to opt into this.



By Dan Raywood

<http://www.scmagazine.com.au/Feature/265065,digital-investigations-have-matured.aspx>

Module Objectives



- Footprinting Terminology
- What Is Footprinting?
- Objectives of Footprinting
- Footprinting Threats
- Footprinting through Search Engines
- Website Footprinting
- Email Footprinting
- Competitive Intelligence
- Footprinting Using Google



- WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites
- Footprinting Tools
- Footprinting Countermeasures
- Footprinting Pen Testing



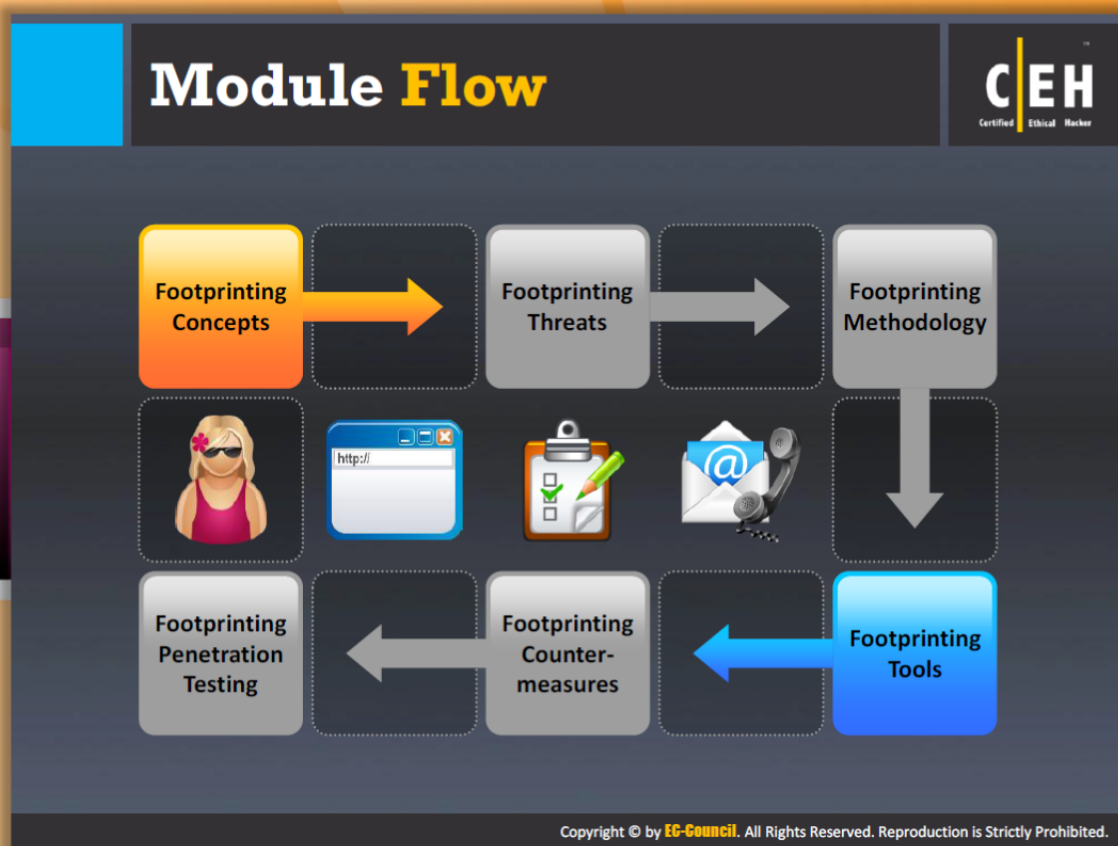
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Module Objectives

This module will make you familiarize with the following:

- Footprinting Terminologies
- What Is Footprinting?
- Objectives of Footprinting
- Footprinting Threats
- Footprinting through Search Engines
- Website Footprinting
- Email Footprinting
- Competitive Intelligence
- Footprinting Using Google
- WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites
- Footprinting Tools
- Footprinting Countermeasures
- Footprinting Pen Testing



Module Flow

Ethical hacking is legal hacking conducted by a penetration tester in order to evaluate the security of an **IT infrastructure** with the permission of an organization. The concept of ethical hacking cannot be explained or cannot be performed in a single step; therefore, it has been divided into several steps. Footprinting is the first step in ethical hacking, where an attacker tries to gather information about a target. To help you better **understand footprinting**, it has been distributed into various sections:

 Footprinting Concepts	 Footprinting Tools
 Footprinting Threats	 Footprinting Countermeasures
 Footprinting Methodology	 Footprinting Penetration Testing

The **Footprinting Concepts** section familiarizes you with footprinting, footprinting terminology, why footprinting is necessary, and the objectives of footprinting.



Footprinting Terminology

Before going deep into the concept, it is important to know the basic terminology used in footprinting. These terms help you understand the concept of footprinting and its structures.



Open Source or Passive Information Gathering

Open source or passive information gathering is the easiest way to collect information about the target organization. It refers to the process of gathering information from the open sources, i.e., publicly available sources. This requires no direct contact with the **target organization**. Open sources may include newspapers, television, social networking sites, blogs, etc.

Using these, you can gather information such as network boundaries, IP address reachable via the Internet, operating systems, web server software used by the target network, TCP and UDP services in each system, access control mechanisms, system architecture, intrusion detection systems, and so on.



Active Information Gathering

In active information gathering, process attackers mainly focus on the employees of

the target organization. Attackers try to extract information from the employees by conducting **social engineering**: on-site visits, interviews, questionnaires, etc.



Anonymous Footprinting

This refers to the process of collecting information from sources anonymously so that your efforts cannot be traced back to you.



Pseudonymous Footprinting

Pseudonymous footprinting refers to the process of collecting information from the sources that have been published on the Internet but is not directly linked to the **author's name**. The information may be published under a different name or the author may have a well-established pen name, or the author may be a corporate or government official and be prohibited from posting under his or her original name. Irrespective of the reason for hiding the author's name, collecting information from such sources is called **pseudonymous**.



Organizational or Private Footprinting

Private footprinting involves collecting information from an organization's **web-based calendar** and email services.



Internet Footprinting

Internet footprinting refers to the process of collecting information of the target organization's connections to the Internet.



What Is Footprinting?

Footprinting, the first step in ethical hacking, refers to the process of collecting information about a target network and its environment. Using footprinting you can find various ways to intrude into the target organization's network system. It is considered "**methodological**" because critical information is sought based on a previous discovery.

Once you begin the footprinting process in a methodological manner, you will obtain the blueprint of the security profile of the target organization. Here the term "**blueprint**" is used because the result that you get at the end of footprinting refers to the unique system profile of the target organization.

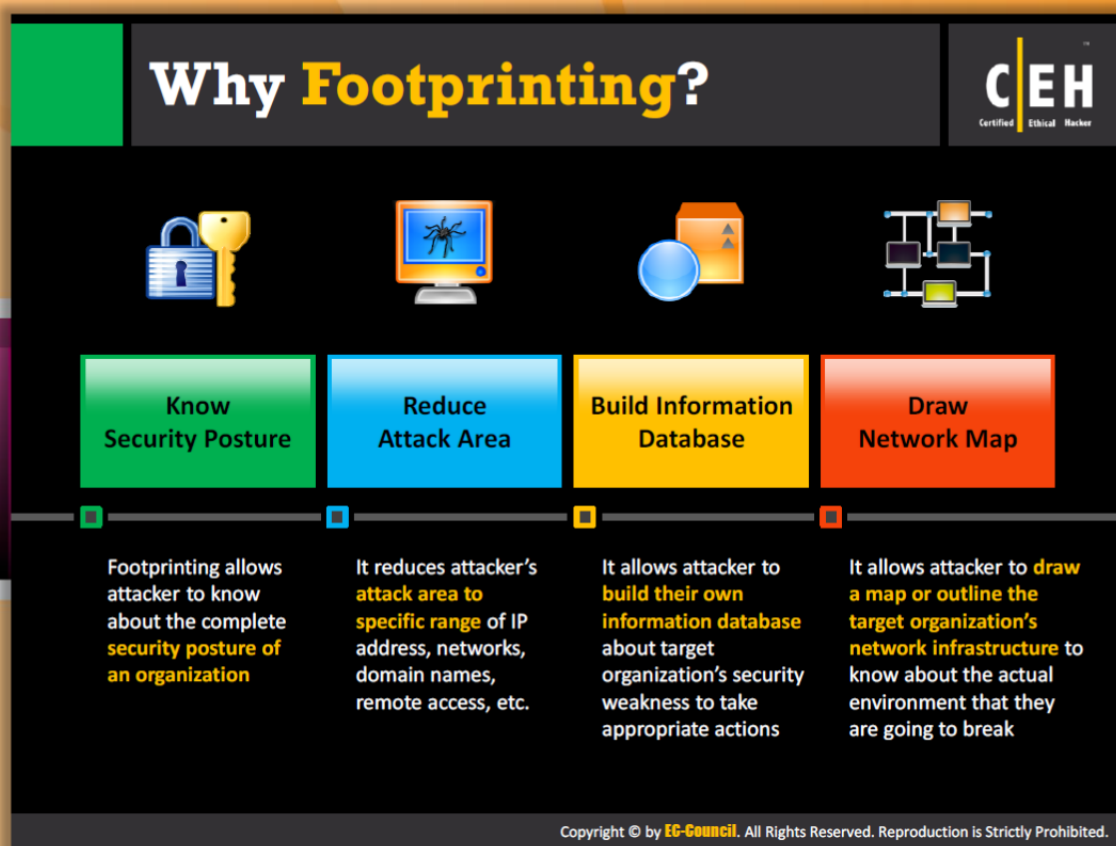
There is no single methodology for footprinting as you can trace information in several routes. However, this activity is important as all crucial information needs to be gathered before you begin hacking. Hence, you should carry out the footprinting precisely and in an **organized manner**.

You can collect information about the target organization through the means of footprinting in four steps:

1. Collect basic information about the target and its network
2. Determine the operating system used, platforms running, web server versions, etc.

3. Perform techniques such as Whois, DNS, network and organizational queries
4. Find vulnerabilities and exploits for launching attacks

Furthermore, we will discuss how to collect basic information, determine operating system of target computer, platforms running, and web server versions, various methods of footprinting, and how to find and **exploit vulnerabilities** in detail.



Why Footprinting?

For attackers to build a hacking strategy, they need to gather information about the target organization's network, so that they can find the easiest way to break into the **organization's security perimeter**. As mentioned previously, footprinting is the easiest way to gather information about the target organization; this plays a vital role in the hacking process.

Footprinting helps to:

- **Know Security Posture**

Performing footprinting on the target organization in a systematic and methodical manner gives the complete profile of the organization's security posture. You can analyze this report to figure out loopholes in the security posture of your target organization and then you can build your **hacking plan** accordingly.

- **Reduce Attack Area**

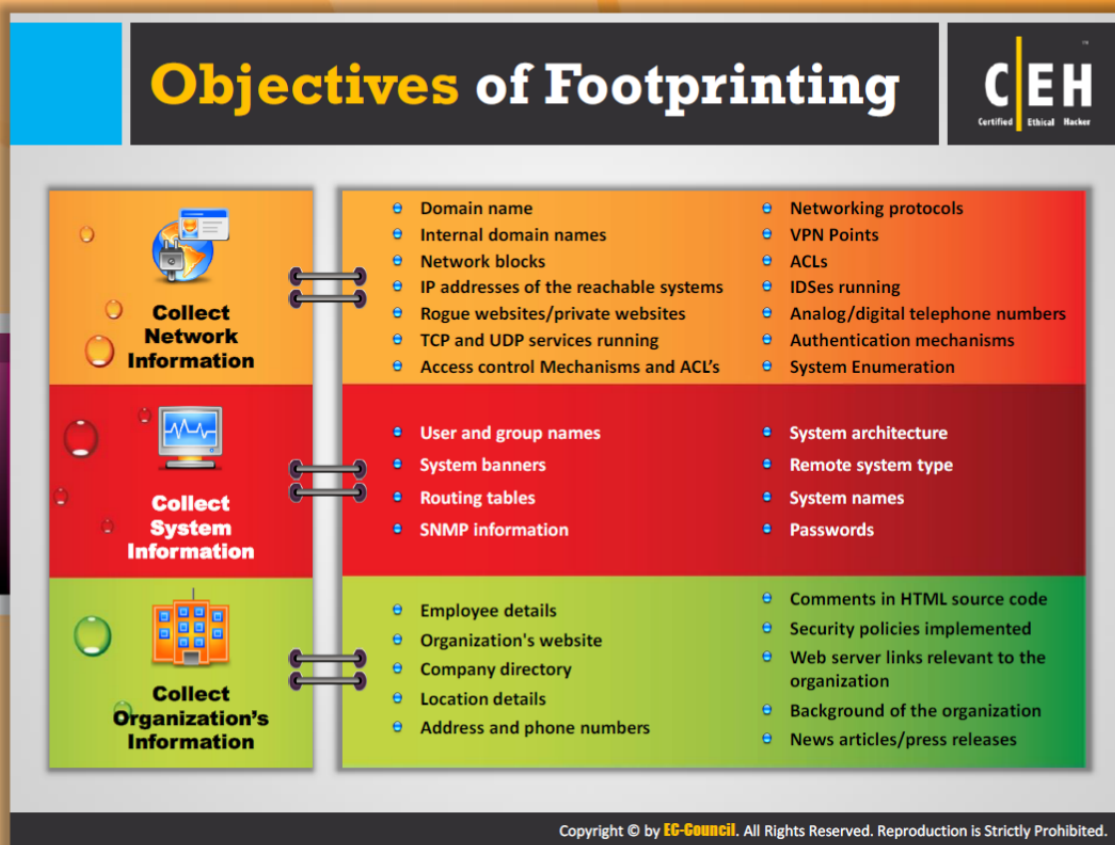
By using a combination of tools and techniques, attackers can take an unknown entity (for example XYZ Organization) and reduce it to a specific range of domain names, network blocks, and individual IP addresses of systems directly connected to the Internet, as well as many other details pertaining to its **security posture**.

- **Build Information Database**

A detailed footprint provides maximum information about the target organization. Attackers can build their own information database about security weakness of the target organization. This database can then be analyzed to find the easiest way to break into the organization's security perimeter.

- **Draw Network Map**

Combining footprinting techniques with tools such as Tracert allows the attacker to create network diagrams of the target organization's network presence. This network map represents their understanding of the **target's Internet footprint**. These network diagrams can guide the attack.



Objectives of Footprinting

The major objectives of footprinting include collecting the **target's network information**, system information, and the organizational information. By carrying out footprinting at various network levels, you can gain information such as: network blocks, network services and applications, system architecture, intrusion detection systems, specific IP addresses, and access control mechanisms. With footprinting, information such as employee names, phone numbers, contact addresses, designation, and work experience, and so on can also be obtained.



Collect Network Information

The network information can be gathered by performing a **Whois database analysis**, **trace routing**, etc. includes:

- Domain name
- Internal domain names
- Network blocks
- IP addresses of the reachable systems
- Rogue websites/private websites

- TCP and UDP services running
- Access control mechanisms and ACLs
- Networking protocols
- VPN points
- ACLs
- IDSes running
- Analog/digital telephone numbers
- Authentication mechanisms
- System enumeration



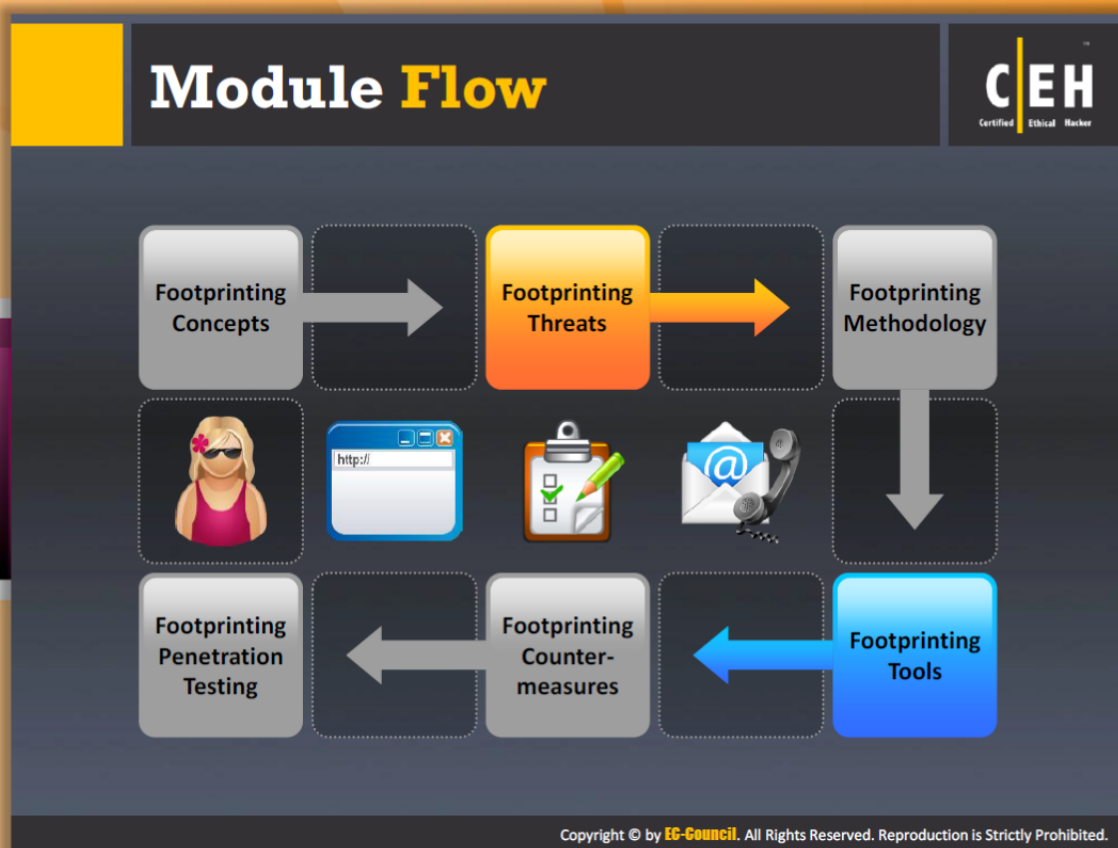
Collect System Information

- User and group names
- System banners
- Routing tables
- SNMP information
- System architecture
- Remote system type
- System names
- Passwords



Collect Organization's Information

- Employee details
- Organization's website
- Company directory
- Location details
- Address and phone numbers
- Comments in HTML source code
- Security policies implemented
- Web server links relevant to the organization
- Background of the organization
- News articles/press releases



Module Flow

So far, we discussed footprinting concepts, and now we will discuss the threats associated with footprinting:

 Footprinting Concepts	 Footprinting Tools
 Footprinting Threats	 Footprinting Countermeasures
 Footprinting Methodology	 Footprinting Penetration Testing

The Footprinting Threats section familiarizes you with the threats associated with footprinting such as social engineering, system and network attacks, corporate espionage, etc.



Footprinting Threats

As discussed previously, attackers perform footprinting as the first step in an attempt to **hack a target organization**. In the footprinting phase, attackers try to collect valuable system-level information such as account details, operating system and other software versions, server names, and database schema details that will be useful in the hacking process.

The following are various threats due to footprinting:



Social Engineering

Without using any intrusion methods, hackers directly and indirectly collect information through persuasion and various other means. Here, crucial information is gathered by the **hackers** through **employees** without their consent.



System and Network Attacks

Footprinting helps an attacker to perform system and network attacks. Through **footprinting**, **attackers** can gather information related to the target organization's system configuration, operating system running on the machine, and so on. Using this information, attackers can find the vulnerabilities present in the target system and then can exploit those

vulnerabilities. Thus, attackers can take control over a target system. Similarly, attackers can also take control over the entire network.



Information Leakage

Information leakage can be a great threat to any organization and is often overlooked. If sensitive organizational information falls into the hands of attackers, then they can build an attack plan based on the information, or use it for **monetary benefits**.



Privacy Loss

With the help of footprinting, hackers are able to access the systems and networks of the company and even escalate the privileges up to admin levels. Whatever **privacy** was maintained by the company is completely lost.



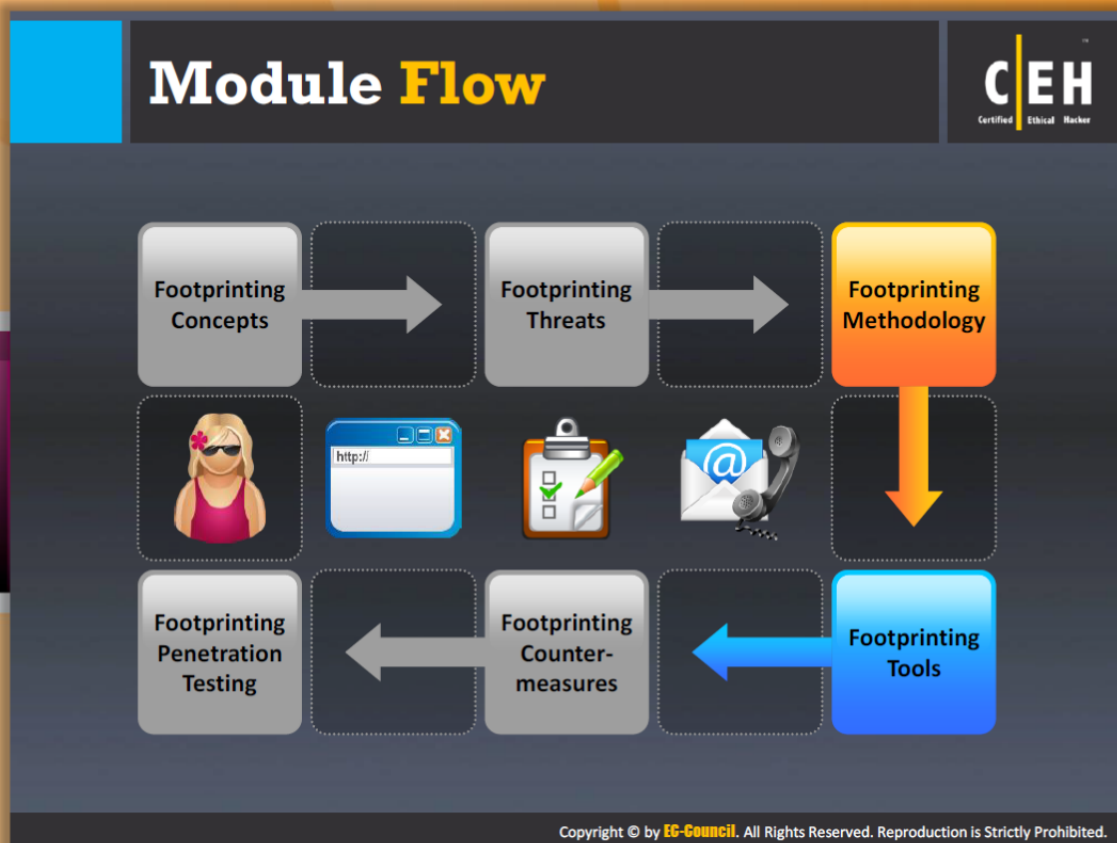
Corporate Espionage

Corporate espionage is one of the major threats to companies as competitors can **spy** and attempt to steal **sensitive data** through footprinting. Due to this type of espionage, competitors are able to launch similar products in the market, affecting the market position of a company.



Business Loss

Footprinting has a major effect on businesses such as online businesses and other **ecommerce websites**, banking and financial related businesses, etc. Billions of dollars are lost every year due to malicious attacks by hackers.



Module Flow

Now that you are familiar with footprinting concepts and threats, we will discuss the footprinting methodology.

The footprinting methodology section discusses various techniques used to collect information about the **target organization** from different sources.

 Footprinting Concepts	 Footprinting Tools
 Footprinting Threats	 Footprinting Countermeasures
 Footprinting Methodology	 Footprinting Penetration Testing



Footprinting Methodology

The footprinting methodology is a procedural way of **collecting information** about a target organization from all available sources. It deals with gathering information about a target organization, determining URL, location, establishment details, number of employees, the specific range of domain names, and contact information. This information can be gathered from various sources such as search engines, Whois databases, etc.

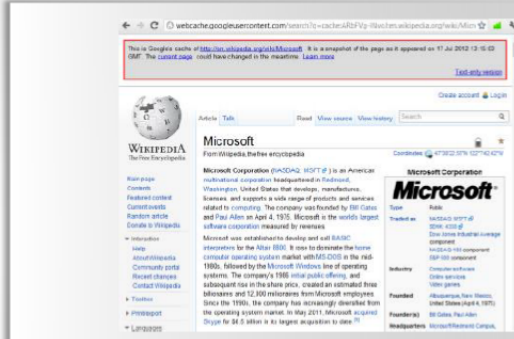
Search engines are the main information sources where you can find valuable information about your **target organization**. Therefore, first we will discuss footprinting through search engines. Here we are going to discuss how and what information we can collect through search engines.

Examples of search engines include: www.google.com, www.yahoo.com, www.bing.com

Footprinting through Search Engines



- Attackers use search engines to **extract information about a target** such as technology platforms, employee details, login pages, intranet portals, etc. which helps in performing social engineering and other types of advanced system attacks
- Search engine **cache may provide sensitive information** that has been removed from the World Wide Web (WWW)



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Footprinting through Search Engines

A web search engine is designed to search for information on the World Wide Web. The search results are generally presented in a line of results often referred to as search engine results pages (SERPs). In the present world, many search engines allow you to extract a target organization's information such as technology platforms, employee details, login pages, intranet portals, and so on. Using this information, an attacker may build a **hacking strategy** to break into the target organization's network and may carry out other types of advanced system attacks. A Google search could reveal submissions to forums by security personnel that reveal brands of firewalls or **antivirus software** in use at the target. Sometimes even network diagrams are found that can guide an attack.

If you want to footprint the target organization, for example XYZ pvt ltd, then type XYZ pvt ltd in the Search box of the search engine and press Enter. This will display all the search results containing the keywords "XYZ pvt ltd." You can even narrow down the results by adding a specific keyword while searching. Furthermore, we will discuss other **footprinting techniques** such as website footprinting and email Footprinting.

For example, consider an organization, perhaps Microsoft. Type Microsoft in the Search box of a search engine and press Enter; this will display all the results containing information about Microsoft. Browsing the results may provide critical information such as **physical location**,

contact address, the services offered, number of employees, etc. that may prove to be a valuable source for hacking.

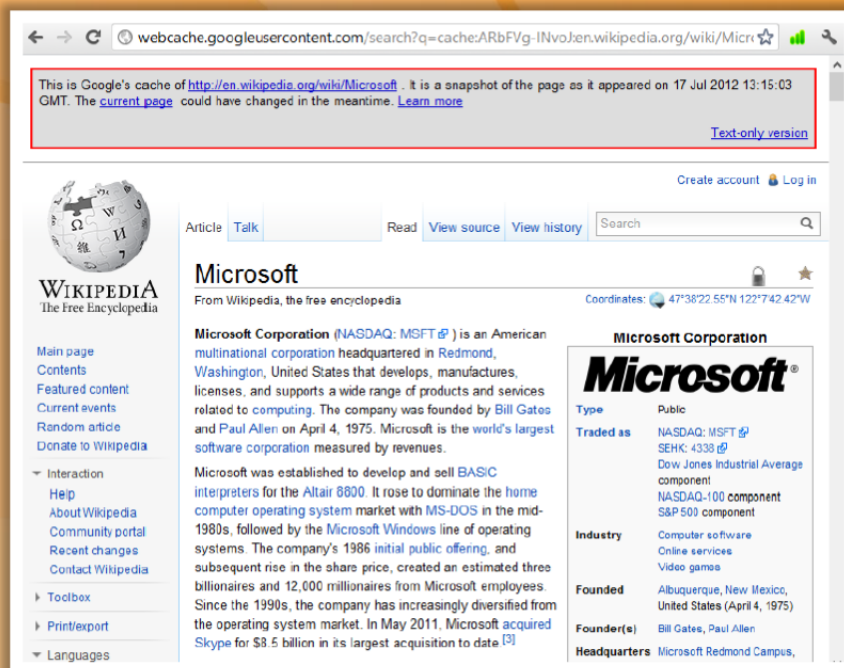


FIGURE 2.1: Screenshot showing information about Microsoft

As an ethical hacker, if you find any **sensitive information** of your company in the search engine result pages, you should remove that information. Although you remove the sensitive information, it may still be available in a search engine cache. Therefore, you should also check the search engine cache to ensure that the sensitive data is removed **permanently**.

Finding Company's External and Internal URLs



- 📌 Search for the target company's external URL in a search engine such as **Google** or **Bing**
- 📌 Internal URLs **provide an insight** into different departments and business units in an organization
- 📌 You may find an internal company's URL by **trial and error method**



Tools to Search Internal URLs

- 🔗 <http://news.netcraft.com>
- 🔗 <http://www.webmaster-a.com/link-extractor-internal.php>



Internal URL's of microsoft.com

- 🔗 support.microsoft.com
- 🔗 office.microsoft.com
- 🔗 search.microsoft.com
- 🔗 msdn.microsoft.com
- 🔗 update.microsoft.com
- 🔗 technet.microsoft.com
- 🔗 windows.microsoft.com



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Finding Company's External and Internal URLs

A company's external and internal URLs provide a lot of useful information to the attacker. These URLs describe the company and provide details such as the company mission and vision, history, products or services offered, etc. The URL that is used **outside the corporate network** for accessing the company's vault server via a firewall is called an external URL. It links directly to the company's external web page. The target company's external URL can be determined with the help of search engines such as **Google** or **Bing**.

If you want to find the external URL of a company, follow these steps:

1. Open any of the search engines, such as Google or Bing.
2. Type the name of the target company in the Search box and press Enter.

The internal URL is used for accessing the company's vault server directly inside the corporate network. The internal URL helps to access the internal functions of a company. Most companies use common formats for internal URLs. Therefore, if you know the **external URL** of a company, you can predict an internal URL through trial and error. These internal URLs provide insight into different departments and business units in an organization. You can also find the internal URLs of an organization using tools such as netcraft.

Tools to Search Internal URLs



Netcraft

Source: <http://news.netcraft.com>

Netcraft deals with web server, web **hosting market-share** analysis, and operating system detection. It provides free anti-phishing toolbar (Net craft toolbar) for Firefox as well as Internet Explorer browsers. The netcraft toolbar avoids phishing attacks and protects the Internet users from fraudsters. It checks the risk rate as well as the hosting location of the websites we visit.



Link Extractor

Source: <http://www.webmaster-a.com/link-extractor-internal.php>

Link Extractor is a link extraction utility that allows you to choose between external and internal URLs, and will return a plain list of URLs linked to or an html list. You can use this utility to **competitor sites**.

Examples of internal URLs of microsoft.com:

- support.microsoft.com
- office.microsoft.com
- search.microsoft.com
- msdn.microsoft.com
- update.microsoft.com
- technet.microsoft.com
- windows.microsoft.com

Public and Restricted Websites

<http://www.microsoft.com>

Public Website

<http://technet.microsoft.com>

<http://windows.microsoft.com>

<http://office.microsoft.com>

<http://answers.microsoft.com>

Restricted Website

Identify a company's **private** and **public** websites

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Public and Restricted Websites

A public website is a website designed to show the presence of an organization on the Internet. It is designed to attract **customers** and **partners**. It contains information such as company history, services and products, and contact information of the organization.

The following screenshot is an example of a public website:

Source: <http://www.microsoft.com>

Module 02 Page 115

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

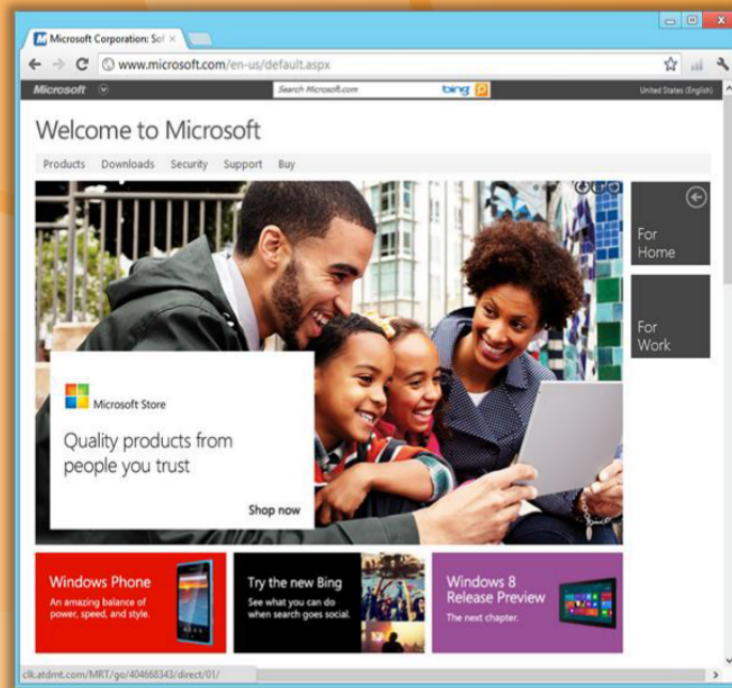


FIGURE 2.2: An example of public website

A restricted website is a website that is available to only a few people. The people may be employees of an organization, members of a department, etc. **Restrictions** can be applied based on the IP number, domain or subnet, username, and password.

Restricted or private websites of microsoft.com include: <http://technet.microsoft.com>, <http://windows.microsoft.com>, <http://office.microsoft.com>, and <http://answers.microsoft.com>.

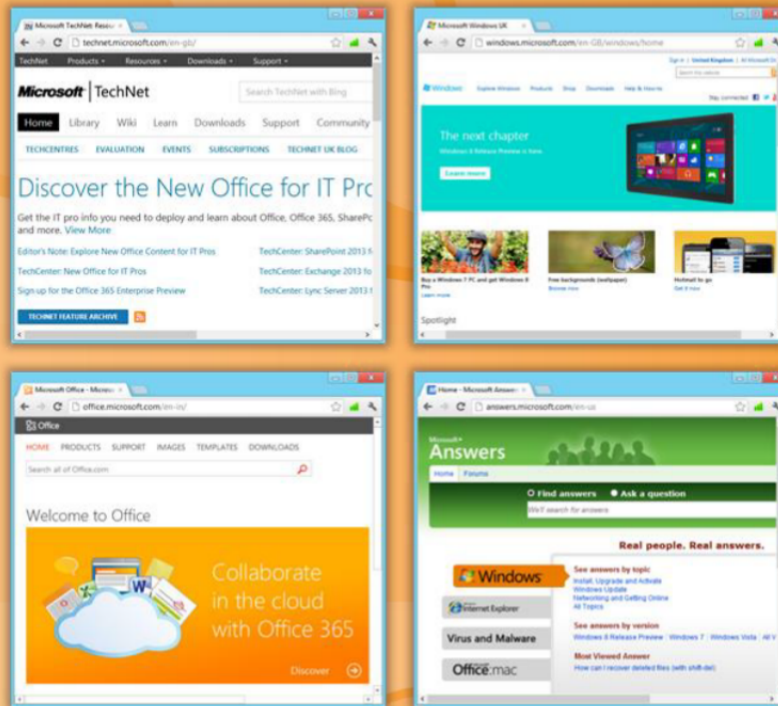
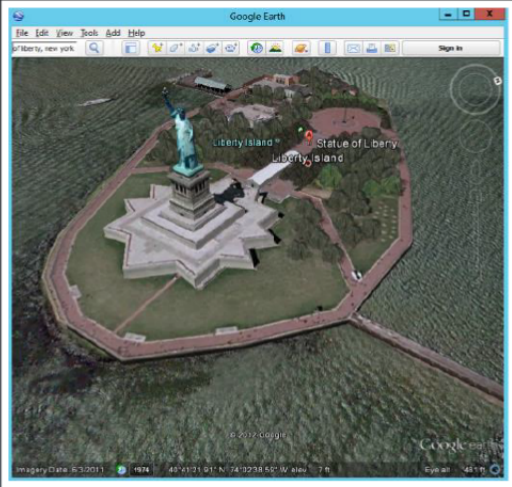
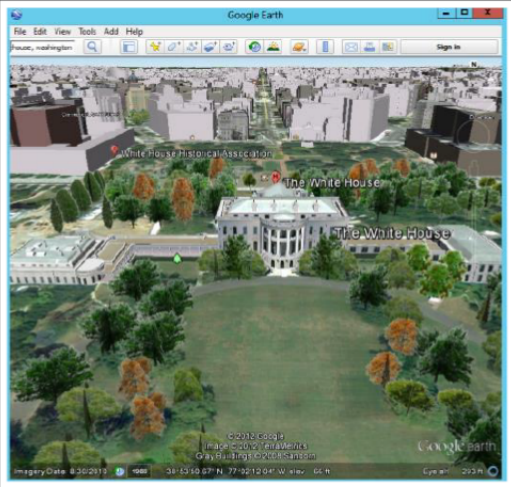


FIGURE 2.3: Examples of Public and Restricted websites

Collect Location Information



<http://earth.google.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Collect Location Information

Information such as physical location of the organization plays a vital role in the hacking process. This information can be obtained using the footprinting technique. In addition to physical location, we can also collect information such as surrounding public Wi-Fi hotspots that may prove to be a way to break into the **target organization's network**.

Attackers with the knowledge of a target organization's location may attempt dumpster diving, surveillance, social engineering, and other non-technical attacks to gather much more information about the target organization. Once the location of the target is known, detailed satellite images of the location can be obtained using various sources available on the Internet such as <http://www.google.com/earth> and <https://maps.google.com>. Attackers can use this information to gain **unauthorized access** to buildings, wired and wireless networks, systems, and so on.

Example: earth.google.com

Google Earth is a valuable tool for **hacking** that allows you to find a location, point, and zoom into that location to explore. You can even **access 3D images** that depict most of the Earth in high-resolution detail.

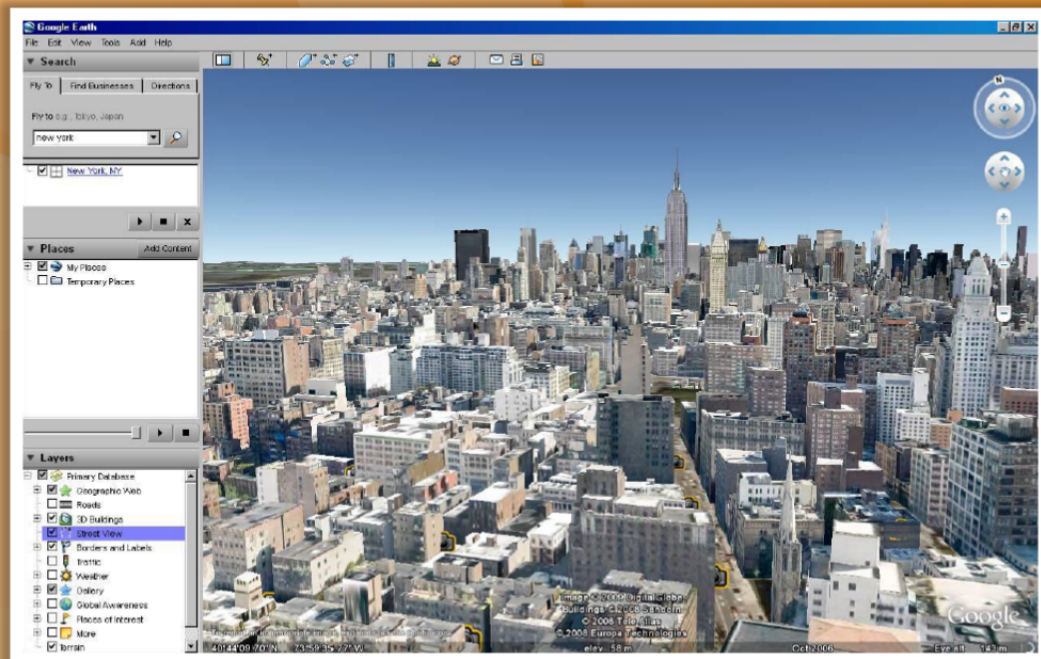


FIGURE 2.4: Google Earth showing location

Example: maps.google.com

Google Maps provides a Street View feature that provides you with a series of images of building, as well as its surroundings, including **Wi-Fi networks**. Attackers may use Google Maps to find or locate entrances to buildings, security cameras, gates, places to hide, weak spots in perimeter fences, and utility resources like electricity connections, to measure distance between different objects, etc.

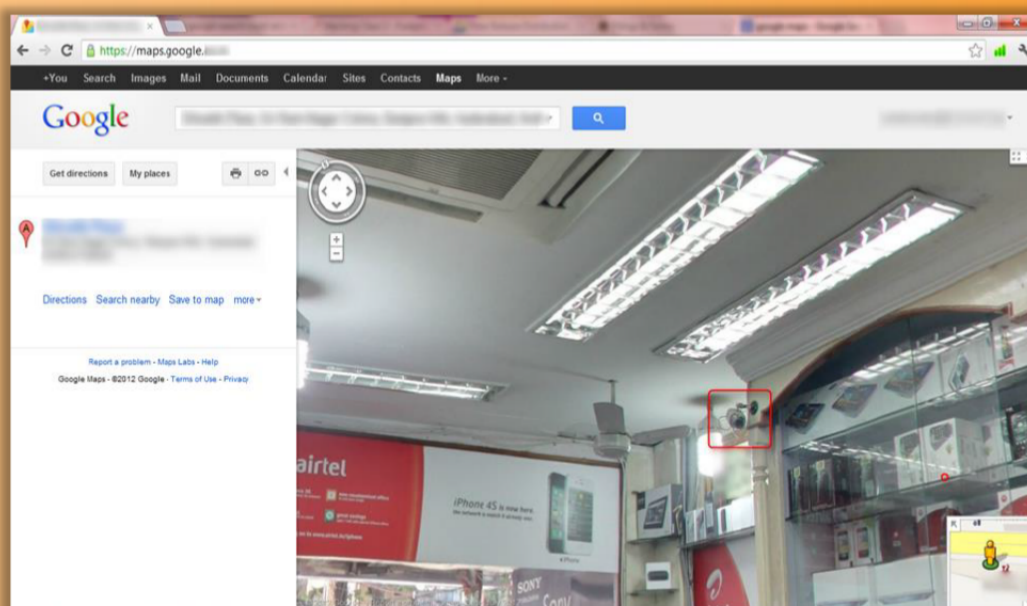


FIGURE 2.5: Google Maps showing a Street View

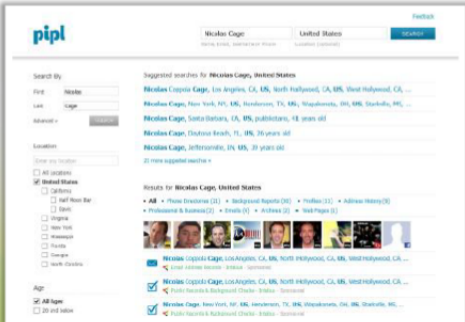
People Search

Information about an individual can be found at various **people search websites**

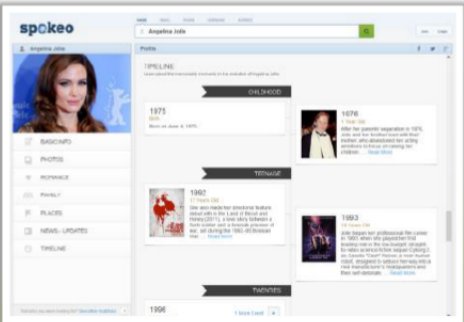


The people search returns the following information about a person:

- Residential addresses and email addresses
- Contact numbers and date of birth
- Photos and social networking profiles
- Blog URLs
- Satellite pictures of private residences



<http://pipl.com>



<http://www.spokeo.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

People Search

You can use the public record websites to find information about people's email addresses, phone numbers, house addresses, and other information. Using this information you can try to obtain bank details, credit card details, mobile numbers, past history, etc. There are many people search online services available that help find people. <http://pipl.com> and <http://www.spokeo.com> are examples of people search services that allow you to search for the people with their name, email, username, phone, or address.

These people search services may provide information such as:

- Residential addresses and email addresses
- Contact numbers and date of birth
- Photos and social networking profiles
- Blog URLs
- Satellite pictures of **private residences**

Module 02 Page 120

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

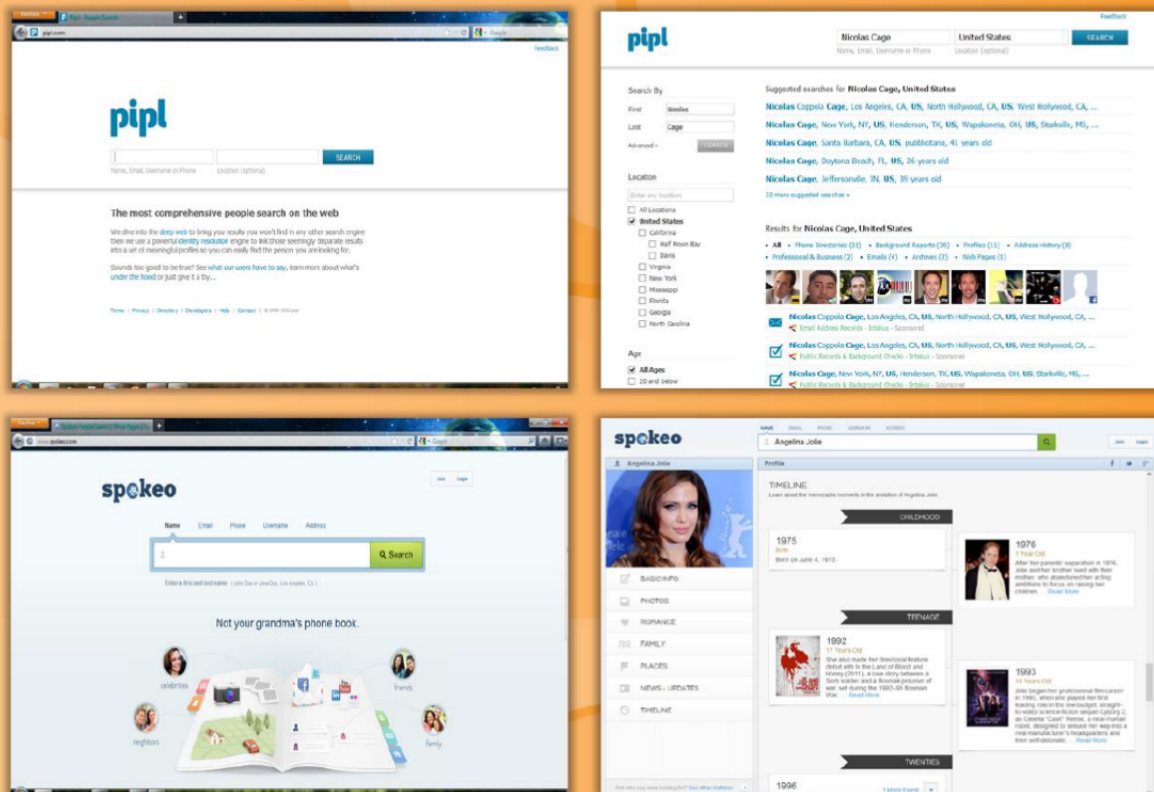


FIGURE 2.6: Examples of People search online service websites

People Search Online Services



 Zaba Search http://www.zabasearch.com	 123 People Search http://www.123people.com
 ZoomInfo http://www.zoominfo.com	 PeekYou http://www.peakyou.com
 Wink People Search http://wink.com	 Intelius http://www.intelius.com
 AnyWho http://www.anywho.com	 PeopleSmart http://www.peoplesmart.com
 People Lookup https://www.peoplelookup.com	 WhitePages http://www.whitepages.com

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



People Search Online Services

At present, many Internet users are using people search engines to find information about other people. Most often people search engines provide **people's names, addresses, and contact details**. Some people search engines may also reveal the type of work an individual does, businesses owned by a person, contact numbers, company email addresses, mobile numbers, fax numbers, dates of birth, personal -mail addresses, etc. This information proves to be highly beneficial for attackers to launch attacks.

Some of the people search engines are listed as follows:



Zaba Search

Source: <http://www.zabasearch.com>

Zaba Search is a people search engine that provides information such as address, phone number, current location, etc. of people in the US. It allows you to search for people by their name.



ZoomInfo

Source: <http://www.zoominfo.com>

Zoom Info is a business people directory using which you can find business contacts, people's professional profiles, biographies, work histories, affiliations, links to **employee profiles** with verified contact information, and more.



Wink People Search

Source: <http://wink.com>

Wink People Search is a people search engine that provides information about people by name and location. It gives phone number, address, websites, photos, work, school, etc.



AnyWho

Source: <http://www.anywho.com>

AnyWho is a website that helps you find information about people, their businesses, and their locations online. With the help of a **phone number**, you can get all the details of an individual.



People Lookup

Source: <https://www.peoplelookup.com>

People Lookup is a people search engine that allows you to find, locate, and then connect with people. It also allows you to look up a phone number, search for cell numbers, find an address or phone number, and search for people in the US. This **database** uses information from **public records**.



123 People Search

Source: <http://www.123people.com>

123 People Search is a people search tool that allows you to find information such as public records, phone numbers, addresses, images, videos, and email addresses.



PeekYou

Source: <http://www.peakyou.com>

PeekYou is a people search engine that allows you to search for profiles and contact information of people in India and cities' top **employers** and **schools**. It allows you to search for the people with their names or usernames.



Intelius

Source: <http://www.intelius.com>

Intelius is a public records business that provides information services. It allows you to search for the people in US with their name, address, phone number, or **email address**.



PeopleSmart

Source: <http://www.peoplesmart.com>

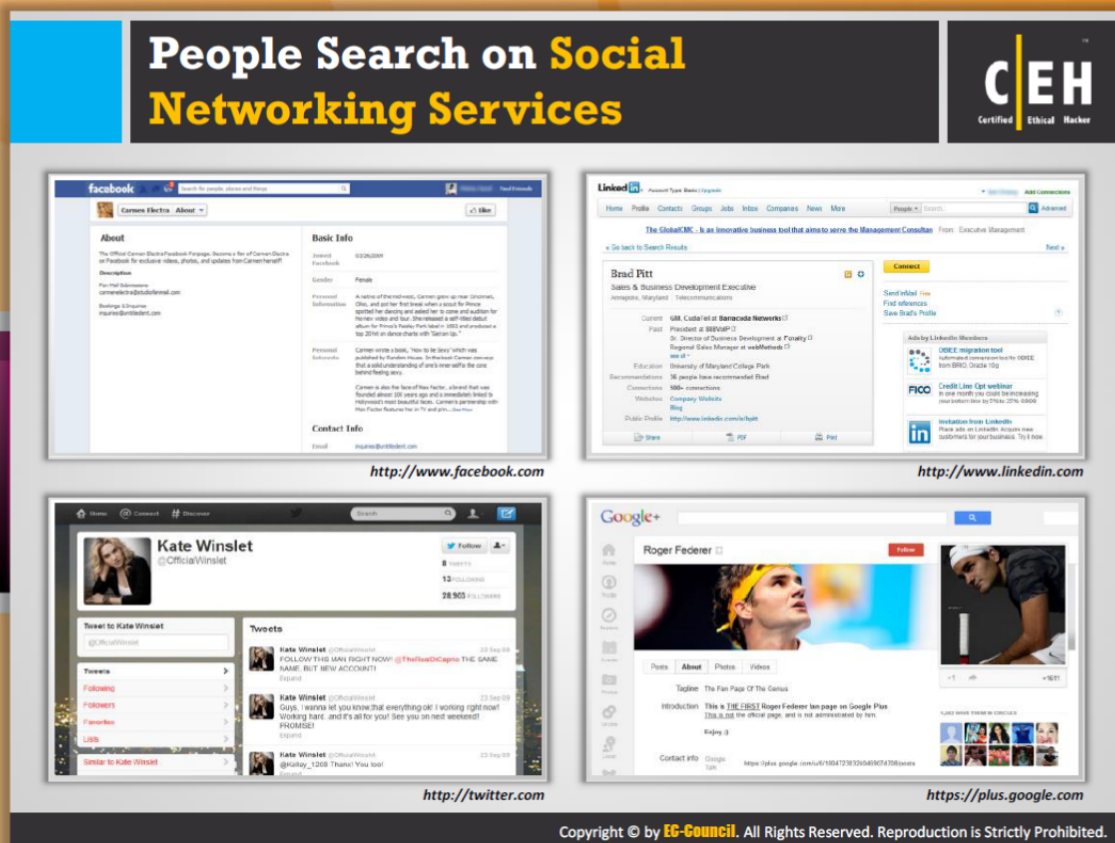
People Smart is a people search service that allows you to find people's work information with their name, city, and state. In addition, it allows you to perform **reverse phone lookups**, email searches, searches by address, and county searches.



WhitePages

Source: <http://www.whitepages.com>

WhitePages is a people search engine that provides information about people by name and location. Using the phone number, you can find the **person's address**.



People Search on Social Networking Services

Searching for people on social networking websites is easy. Social networking services are the online services, platforms, or sites that focus on facilitating the building of social networks or social relations among people. These websites provide information that is provided by users. Here, people are directly or indirectly related to each other by **common interest**, work location, or educational communities, etc.

Social networking sites allow people to share information quickly and effectively as these sites are updated in real time. It allows updating facts about upcoming or current events, recent announcements and invitations, and so on. Therefore, social networking sites prove to be a great platform for searching people and their related information. Through people searching on **social networking services**, you can gather critical information that will be helpful in performing social engineering or other kinds of attacks.

Many social networking sites allow visitors to search for people without registration; this makes people searching on social networking sites an easy task for you. You can search a person using name, email, or address. Some sites allow you to check whether an account is currently in use or not. This allows you to check the status of the person you are looking for.

Some of social networking services are as follows:



Facebook

Source: <http://www.facebook.com>

Facebook allows you to search for people, their **friends**, **colleagues**, and **people** living around them and others with whom they are affiliated. In addition, you can also find their professional information such as their company or business, current location, phone number, email ID, photos, videos, etc. It allows you to search for people by username or email address.

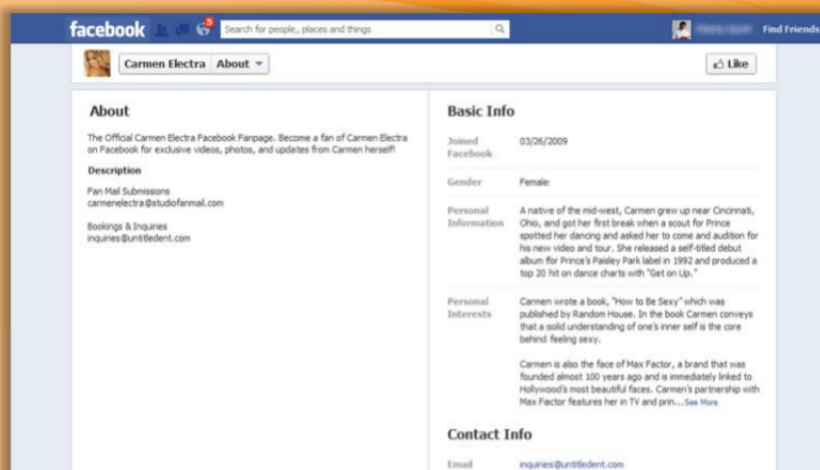


FIGURE 2.7: Facebook a social networking service to search for people across the world



LinkedIn

Source: <http://www.linkedin.com>

LinkedIn is a **social networking website** for professional people. It allows you to find people by name, keyword, company, school, etc. Searching for people on LinkedIn gives you information such as name, designation, name of company, current location, and education qualifications, but to use LinkedIn you need to be registered with the site.

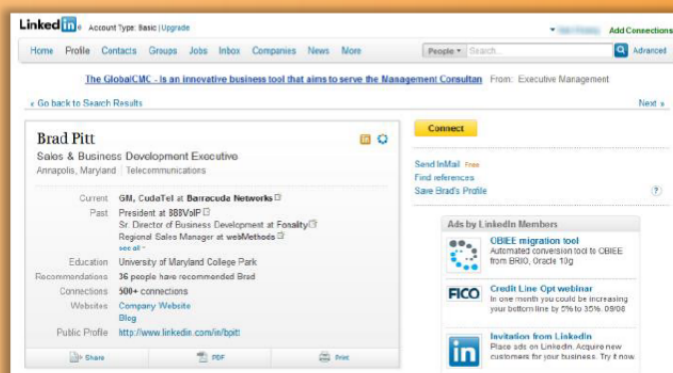


FIGURE 2.8: LinkedIn screenshot



Twitter

Source: <http://twitter.com>

Twitter is a social networking service that allows people to send and **read text messages** (tweets). Even unregistered users can read tweets on this site.

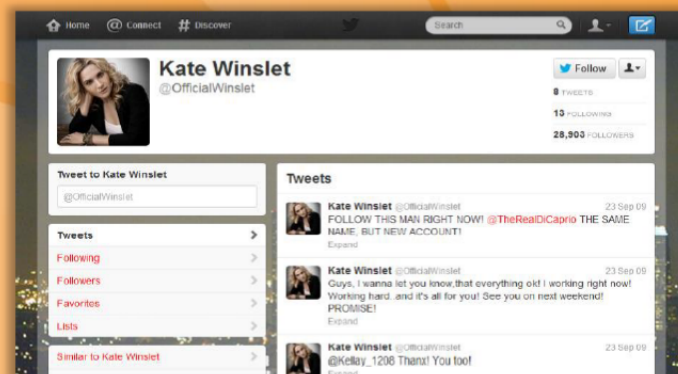


FIGURE 2.9: Twitter screenshot

Google+

Source: <https://plus.google.com>

Google+ is a social networking site that aims to make sharing on the web more like **sharing in real life**. You can grab a lot of useful information about users from this site and use it to hack their systems.

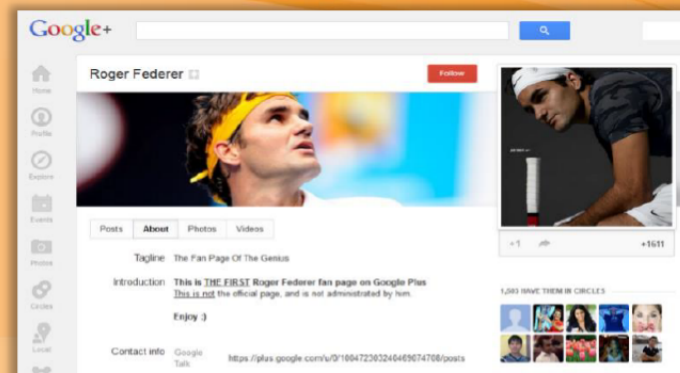


FIGURE 2.10: Google+ screenshot



Gather Information from Financial Services

Financial services such as Google Finance, Yahoo! Finance, and so on provide a lot of useful information such as the market value of a company's shares, company profile, competitor details, etc. The information offered varies from one service to the next. In order to avail themselves of services such as e-mail alerts and phone alerts, users need to register on the financial services. This gives an opportunity for an attacker to **grab useful information for hacking**.

Many financial firms rely on web access, performing transactions, and user access to their accounts. Attackers can obtain sensitive and private information of users using information theft, key loggers, etc. Attackers can even grab this information by implementing cybercrimes, and exploit it with the help of non-vulnerable threats (software design flaw example; breaking authentication mechanism).

The following are some of non-vulnerable threats:

- Service flooding
- Brute force attack
- Phishing

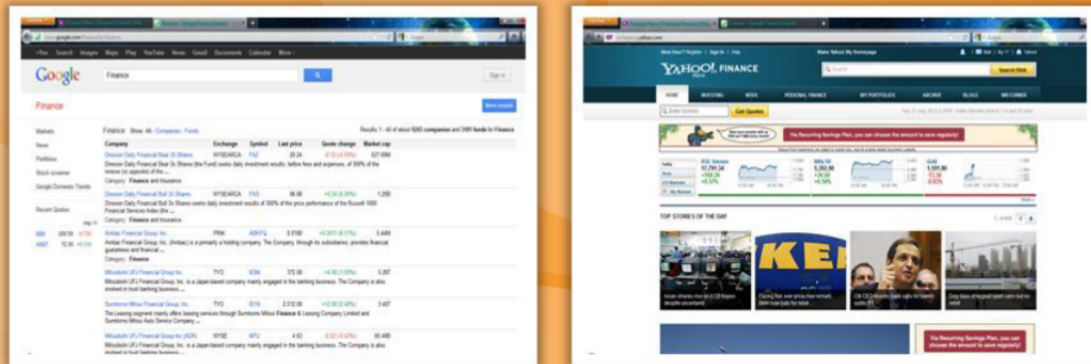


FIGURE 2.11: Examples of financial services website for gathering information

Footprinting through Job Sites





You can gather company's infrastructure details from job postings

Enterprise Applications Engineer/DBA

About Us:
Since 1984, the World & Brown Family of Companies have been connecting business to industry-leading solutions in every area of health insurance and benefits services. We've built a reputation for providing leaders, careers, employees, individuals and families with access to the services, tools and technology that help them succeed. We call it providing, "Service of Unequalled Excellence."

We extend this same level of service to our most important asset: our employees! We offer competitive salaries and benefits, but our strength is our family culture. We foster a casual but hard working environment, organize fun monthly events and regularly recognize our employees through a variety of programs. We provide in-house corporate training to sharpen skills so our employees are not only successful in their current jobs, but can follow a career path. We take pride in promoting from within!

If this is the kind of family you would like to be a part of, please check out this employment opportunity and join our team!

Job Description:
The Enterprise Applications Engineer's role is to plan, implement, manage, administer and support core business applications software for corporate enterprise needs. This includes, but is not limited to: Microsoft SQL Server, Microsoft Exchange 2010 and Unified Messaging, Microsoft SharePoint, Microsoft Great Plains, Microsoft CRM, Microsoft SCL Server 2005 and 2008, Microsoft Team Foundation Server 2008 and 2010, Microsoft SCCM, proprietary developed software and open source applications utilized by the company.

Job Knowledge and Skills:
Position requires strong knowledge of Windows server 2003/2008 Active Directory administration and networking (TCP/IP, DNS and DHCP). Must have experience with and strong working knowledge of Microsoft SQL 2005 and 2008, Microsoft Exchange 2010 messaging systems, Microsoft SharePoint, Microsoft CRM and Microsoft SCCM. Must have basic programming and scripting skills. Proficient in C# and Powershell scripting experience. Must be knowledgeable of server class hardware and Network infrastructure best practices. MCTS, MCSE, MCITP, SQL, etc. and/or MCTS, MCSE certification preferred. Bachelor degree in Computer Science or Network Engineering, professional training or equivalent experience.

Look for these:

- Job requirements
- Employee's profile
- Hardware information
- Software information



Examples of Job Websites

- <http://www.monster.com>
- <http://www.careerbuilder.com>
- <http://www.dice.com>
- <http://www.simplyhired.com>
- <http://www.indeed.com>
- <http://www.usajobs.gov>



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Footprinting through Job Sites

Attackers can gather valuable information about the operating system, software versions, company's infrastructure details, and **database schema** of an organization, through footprinting various job sites using different techniques. Depending upon the posted requirements for job openings, attackers may be able to study the hardware, network-related information, and technologies used by the company. Most of the company's websites have a key employees list with their email addresses. This information may prove to be beneficial for an attacker. For example, if a company wants to hire a person for a **Network Administration job**, it posts the requirements related to that position.

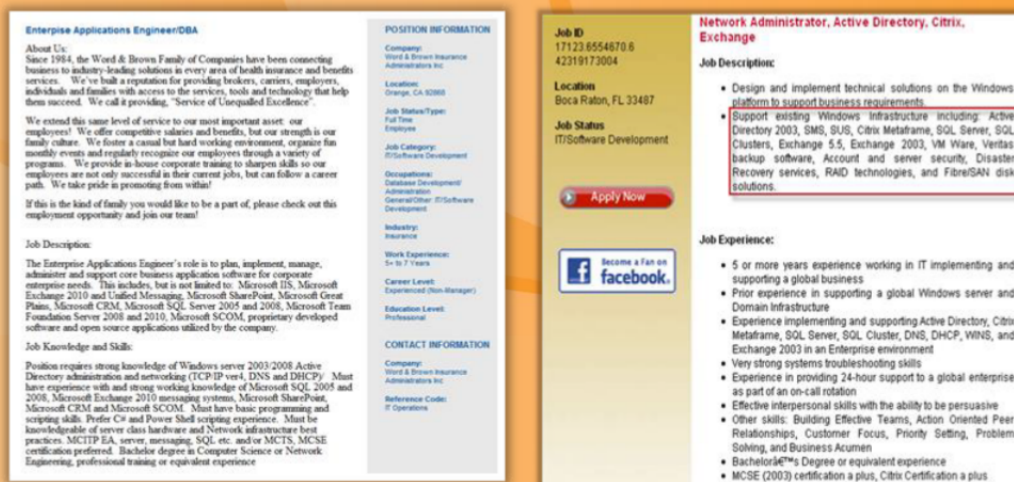


FIGURE 2.12: Gathering information through Job websites

Usually attackers look for the following information:

- Job requirements
- Employee's profile
- Hardware information
- Software information

Examples of job websites include:

- <http://www.monster.com>
- <http://www.careerbuilder.com>
- <http://www.dice.com>
- <http://www.simplyhired.com>
- <http://www.indeed.com>
- <http://www.usajobs.gov>

Monitoring Target Using Alerts

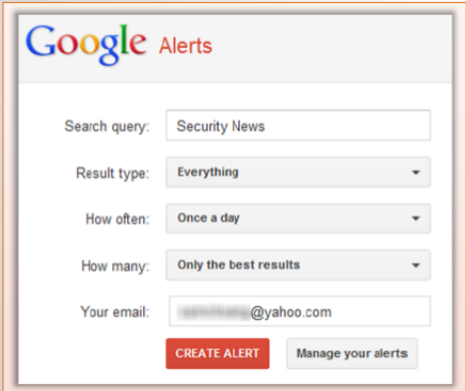


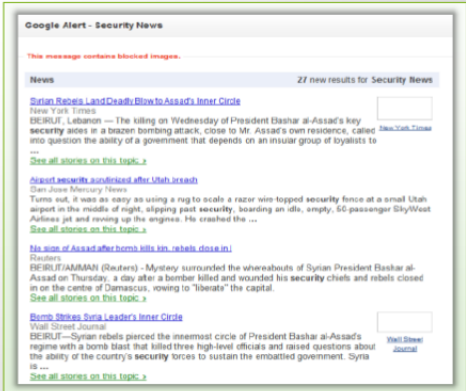
Alerts are the **content monitoring services** that provide up-to-date information based on your preference usually via **email** or **SMS** in an automated manner

Examples of Alert Services

- Google Alerts - <http://www.google.com/alerts>
- Yahoo! Alerts - <http://alerts.yahoo.com>
- Giga Alert - <http://www.gigaalert.com>







Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Monitoring Targets Using Alerts

Alerts are the content monitoring services that provide automated up-to-date information based on your preference, usually via **email** or **SMS**. In order to get alerts, you need to register on the website and you should submit either an email or phone number to the service. Attackers can gather this sensitive information from the **alert services** and use it for further processing of an attack.



Google Alerts

Source: <http://www.google.com/alerts>

Google Alerts is a content monitoring service that automatically notifies users when new content from news, web, blogs, video, and/or discussion groups matches a set of search terms selected by the user and stored by the Google Alerts service.

Google Alerts aids in monitoring a developing news story and keeping current on a **competitor** or **industry**.

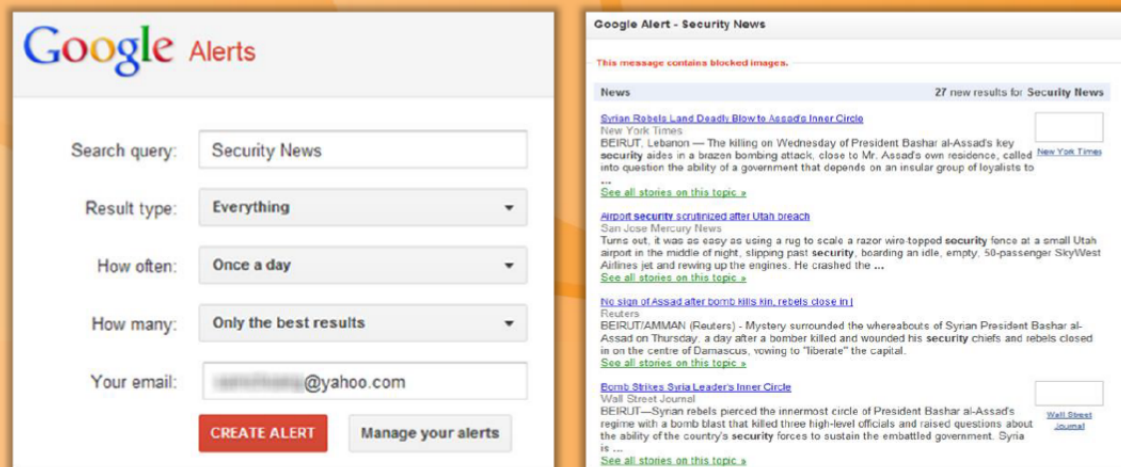


FIGURE 2.13: Google Alert services screenshot

Yahoo! Alerts is available at <http://alerts.yahoo.com> and Giga Alert is available at <http://www.gigaalert.com>; these are two more examples of alert services.



Footprinting Methodology

So far, we have discussed the first step of footprinting methodology, i.e., footprinting via search engines. Now we will discuss website footprinting. An **organization's website** is a first place where you can get sensitive information such as names and contact details of chief persons in the company, upcoming project details, and so on. This section covers the website footprinting concept, mirroring websites, the tools used for mirroring, and **monitoring web updates**.

Website Footprinting



Information obtained from target's website enables an attacker to build a detailed **map of website's structure and architecture**

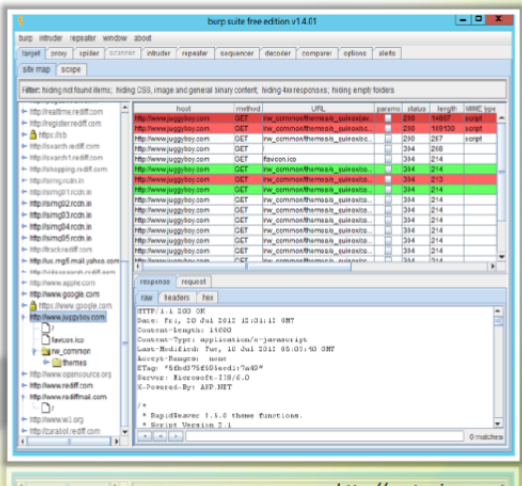


Browsing the target website may provide:

- Software used and its version
- Operating system used
- Sub-directories and parameters
- Filename, path, database field name, or query
- Scripting platform
- Contact details and CMS details

Use Zaproxy, Burp Suite, Firebug, etc. to view headers that provide:

- Connection status and content-type
- Accept-Ranges
- Last-Modified information
- X-Powered-By information
- Web server in use and its version



http://portswigger.net

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Website Footprinting

It is possible for an attacker to build a detailed map of a website's structure and architecture without IDS being triggered or without raising any sys admin suspicions. It can be accomplished either with the help of sophisticated footprinting tools or just with the basic tools that come along with the operating system, such as **telnet** and a **browser**.

Using the **Netcraft tool** you can gather website information such as IP address, registered name and address of the domain owner, domain name, host of the site, OS details, etc. But this tool may not give all these details for every site. In such cases, you should browse the target website.

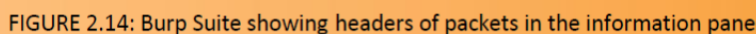
Browsing the target website will provide you with the following information:

- Software used and its version: You can find not only the software in use but also the version easily on the off-the-shelf **software-based** website.
- Operating system used: Usually the operating system can also be determined.
- Sub-directories and parameters: You can reveal the **sub-directories** and parameters by making a note of all the URLs while browsing the target website.

- CMS software** allows URL rewriting in order to disguise the script filename extensions. In this case, you need to put little more effort to determine the scripting platform.

- Connection status and content-type
- Accept-ranges
- Last-Modified information
- X-Powered-By information
- Web server in use and its version

The following is a screenshot of Burp Suite showing headers of packets in the information pane:



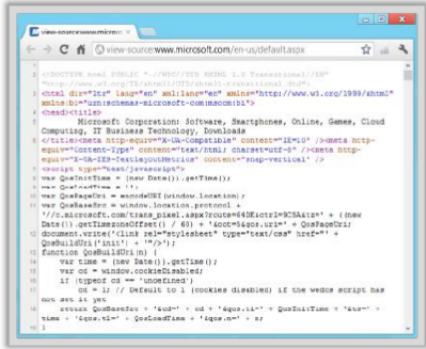
Website Footprinting

(Cont'd)



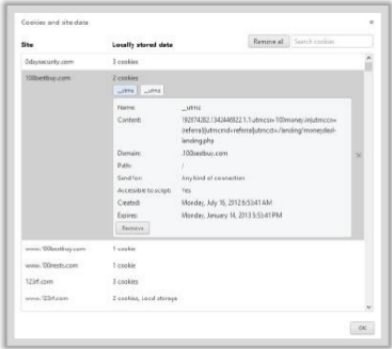
Examining HTML source provides:

- Comments in the source code
- Contact details of web developer or admin
- File system structure
- Script type



Examining cookies may provide:

- Software in use and its behavior
- Scripting platforms used

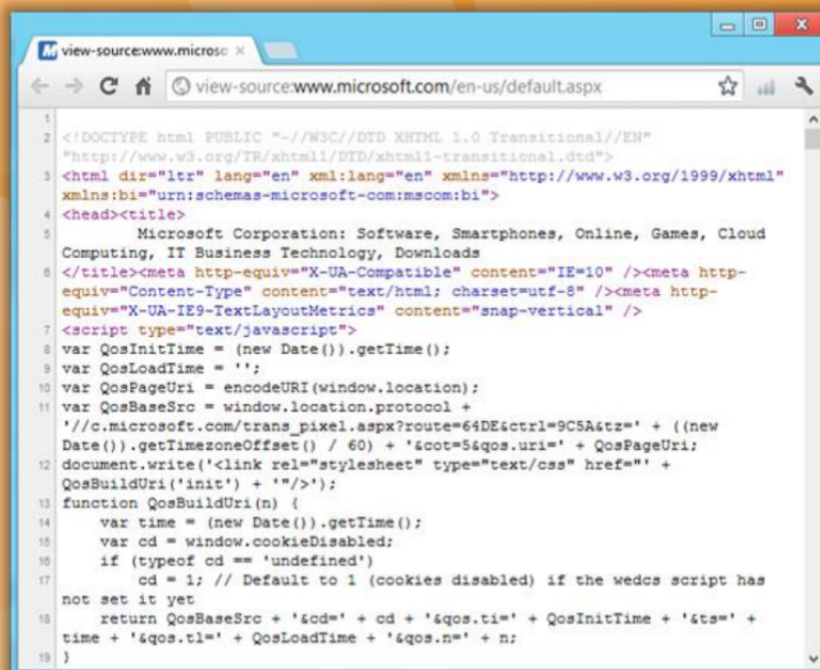
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Website Footprinting (Cont'd)

Examine the **HTML source code**. Follow the comments that are either created by the CMS system or inserted manually. These comments may provide clues to help you understand what's running in the background. This may even provide contact details of the web admin or developer.

Observe all the links and image tags, in order to map the file system structure. This allows you to reveal the existence of hidden directories and files. Enter **fake data** to determine how the script works.



```

1 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
2 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
3 <html dir="ltr" lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml"
4 xmlns:bi="urn:schemas-microsoft-com:mscom:bi">
5 <head><title>
6 Microsoft Corporation: Software, Smartphones, Online, Games, Cloud
7 Computing, IT Business Technology, Downloads
8 </title><meta http-equiv="X-UA-Compatible" content="IE=10" /><meta http-
9 equiv="Content-Type" content="text/html; charset=utf-8" /><meta http-
10 equiv="X-UA-IE9-TextLayoutMetrics" content="snap-vertical" />
11 <script type="text/javascript">
12 var QoSInitTime = (new Date()).getTime();
13 var QoSLoadTime = '';
14 var QoSPageUri = encodeURIComponent(window.location);
15 var QoSBaseSrc = window.location.protocol +
16 '//c.microsoft.com/trans_pixel.aspx?route=64DE&ctrl=9CSA&tz=' + ((new
17 Date()).getTimezoneOffset() / 60) + '&cot=5&qos.uri=' + QoSPageUri;
18 document.write('<link rel="stylesheet" type="text/css" href="' +
19 QoSBuildUri('init') + '>');
20 function QoSBuildUri(n) {
21     var time = (new Date()).getTime();
22     var cd = window.cookieDisabled;
23     if (typeof cd == 'undefined')
24         cd = 1; // Default to 1 (cookies disabled) if the wedcs script has
25 not set it yet
26     return QoSBaseSrc + '&cd=' + cd + '&qos.ti=' + QoSInitTime + '&ts=' +
27 time + '&qos.tl=' + QoSLoadTime + '&qos.n=' + n;
28 }

```

FIGURE 2.15: Screenshot showing Microsoft script works

Examine cookies set by the server to determine the software running and its behavior. You can also identify the script in platforms by observing sessions and other supporting **cookies**.

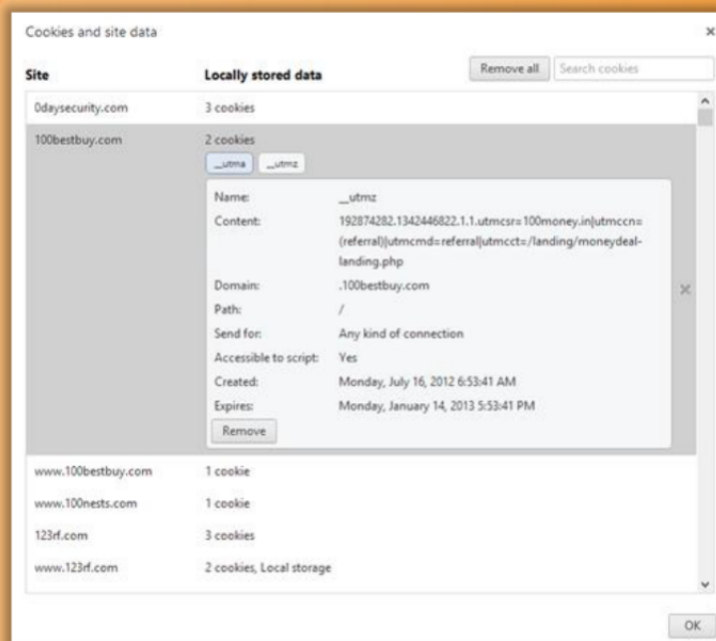


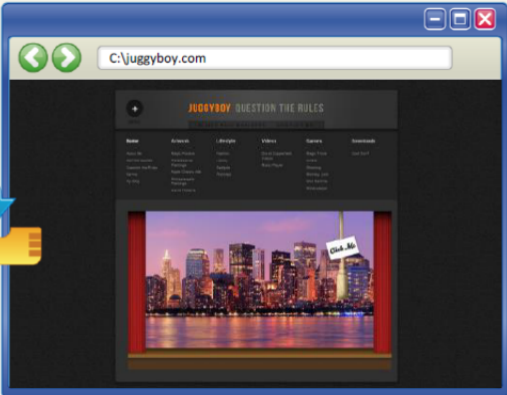
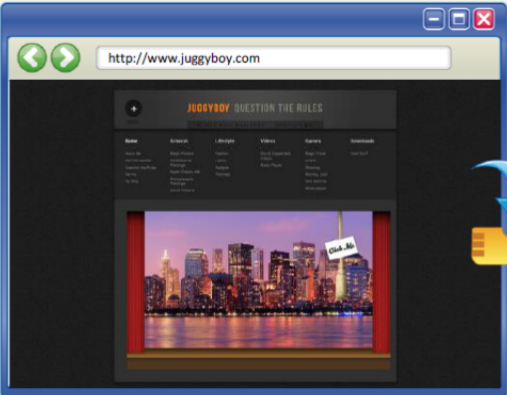
FIGURE 2.16: Showing details about the software running in a system by examining cookies

Mirroring Entire Website



- Mirroring an entire website onto the local system enables an attacker to **dissect and identify vulnerabilities**; it also assists in finding **directory structure** and other valuable information without multiple requests to web server
- Web mirroring tools allow you to **download a website to a local directory**, building recursively all directories, HTML, images, flash, videos, and other files from the server to your computer





Original Website **Mirrored Website**

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Mirroring an Entire Website

Website mirroring is the process of creating an exact replica of the original website. This can be done with the help of web mirroring tools. These tools allow you to download a website to a local directory, recursively building all **directories, HTML, images, flash, videos** and other files from the server to your computer.

Website mirroring has the following benefits:

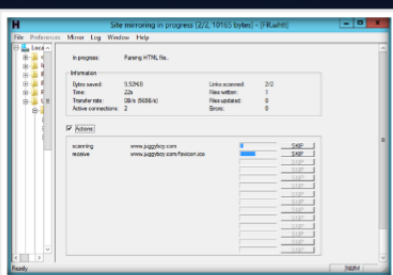
- It is helpful for offline site browsing.
- Website mirroring helps in creating a backup site for the original one.
- A website clone can be created.
- Website mirroring is useful to test the site at the time of website design and development.
- It is possible to distribute to **multiple servers** instead of using only one server.



FIGURE 2.17: JuggyBoy's Original and Mirrored website

Website Mirroring Tools

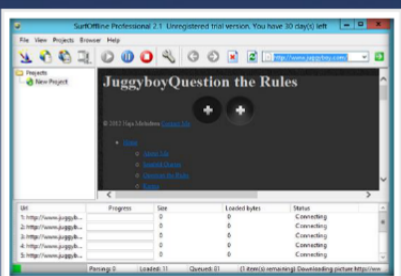




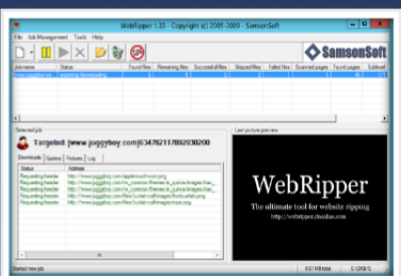
HTTrack Web Site Copier (<http://www.httrack.com>)



BlackWidow (<http://softbytelabs.com>)



SurfOffline (<http://www.surfoffline.com>)



WebRipper (<http://www.calluna-software.com>)

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Website Mirroring Tools



HTTrack Web Site Copier

Source: <http://www.httrack.com>

HTTrack is an offline browser utility. It allows you to download a World Wide Web site from the Internet to a **local directory**, building recursively all directories, getting HTML, images, and other files from the server to your computer. HTTrack arranges the original **site's relative link-structure**. Open a page of the "mirrored" website in your browser, browse the site from link to link, and you can view the site as if you were online. HTTrack can also update an existing mirrored site, and resume interrupted downloads.

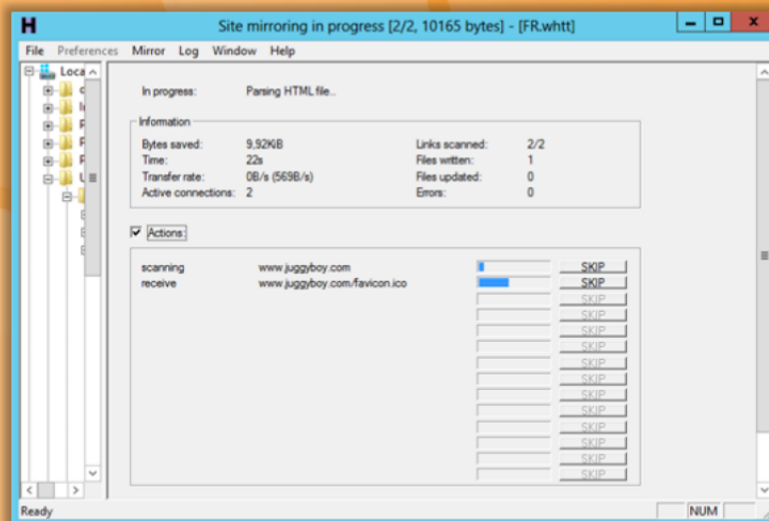


FIGURE 2.18: HTTrack Web Site Copier Screenshot



SurfOffline

Source: <http://www.surfoffline.com>

SurfOffline is a website download **software**. The software allows you to download entire websites and download web pages to your local hard drive. After downloading the target website, you can use SurfOffline as an offline browser and view downloaded web pages in it. If you prefer to view downloaded webpages in another browser, you can use the **Export Wizard**.

SurfOffline's Export Wizard also allows you to copy downloaded websites to other computers in order to view them later and prepares websites for burning them to a CD or DVD.

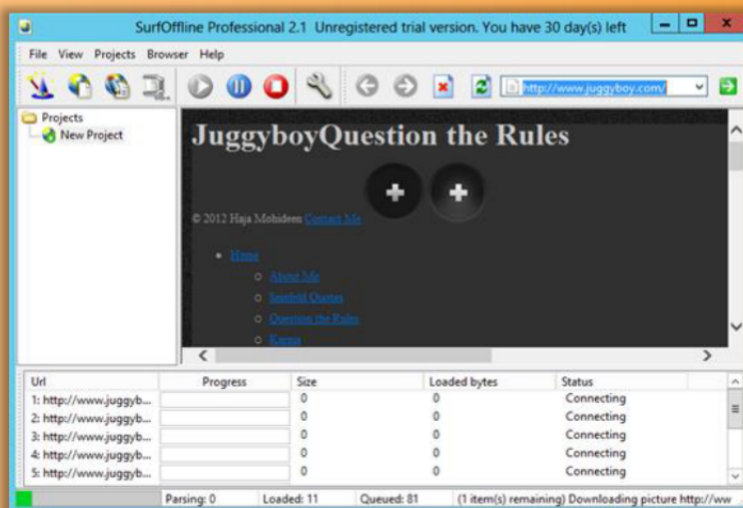


FIGURE 2.19: SurfOffline screenshot



BlackWidow

Source: <http://softbytelabs.com>

BlackWidow is a website scanner for both experts and beginners. It scans websites (it's a site ripper). It can download an entire website or part of a website. It will build a site structure first, and then downloads. It allows you to choose what to download from the website.



FIGURE 2.20: SurfOffline screenshot



Webripper

Source: <http://www.calluna-software.com>

WebRipper is an Internet scanner and downloader. It downloads massive amount of images, videos, audio, and executable documents from any website. WebRipper uses **spider-technology** to follow the links in all directions from the start-address. It filters out the interesting files, and adds them to the download-queue for downloading.

You can restrict downloaded items by file type, minimum file, maximum file, and image size. All the downloaded links can also be restricted by keywords to avoid wasting your **bandwidth**.

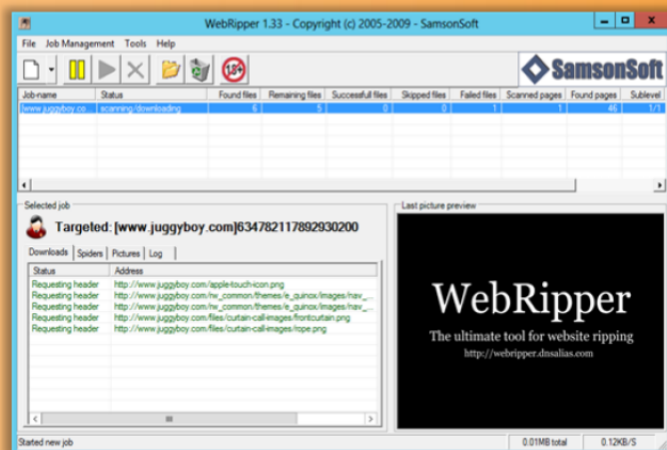


FIGURE 2.21: Webripper screenshot

Website Mirroring Tools (Cont'd)



 Website Ripper Copier http://www.tensons.com	 PageNest http://www.pagenest.com
 Teleport Pro http://www.tenmax.com	 Backstreet Browser http://www.spadixbd.com
 Portable Offline Browser http://www.metaproducts.com	 Offline Explorer Enterprise http://www.metaproducts.com
 Proxy Offline Browser http://www.proxy-offline-browser.com	 GNU Wget http://www.gnu.org
 iMiser http://internetresearchtool.com	 Hooeey Webprint http://www.hooeeywebprint.com

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Website Mirroring Tools (Cont'd)

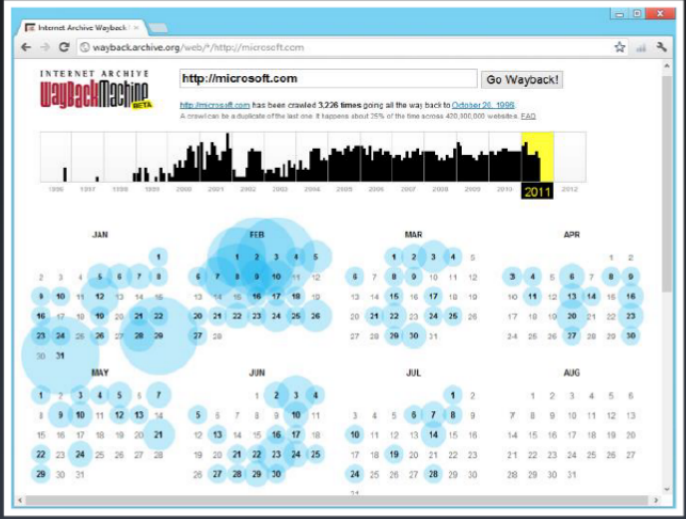
In addition to the website mirroring tools mentioned previously, a few more well-known tools are mentioned as follows:

- Website Ripper Copier available at <http://www.tensons.com>
- Teleport Pro available at <http://www.tenmax.com>
- Portable Offline Browser available at <http://www.metaproducts.com>
- Proxy Offline Browser available at <http://www.proxy-offline-browser.com>
- iMiser available at <http://internetresearchtool.com>
- PageNest available at <http://www.pagenest.com>
- Backstreet Browser available at <http://www.spadixbd.com>
- Offline Explorer Enterprise available at <http://www.metaproducts.com>
- GNU Wget available at <http://www.gnu.org>
- Hooeey Webprint available at <http://www.hooeeywebprint.com>

Extract Website Information from <http://www.archive.org>



Internet Archive's Wayback Machine allows you to visit **archived** versions of websites



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Extract Website Information from <http://www.archive.org>

Archive is an **Internet Archive Wayback Machine** that allows you to visit archived versions of websites. This allows you to gather information on a company's web pages since their creation. As the website www.archive.org keeps track of web pages from the time of their inception, you can retrieve even information that has been removed from the **target website**.

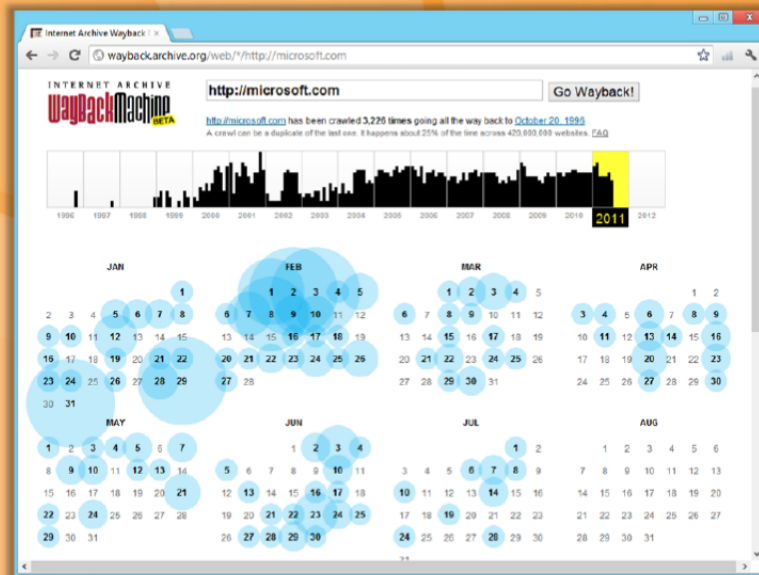
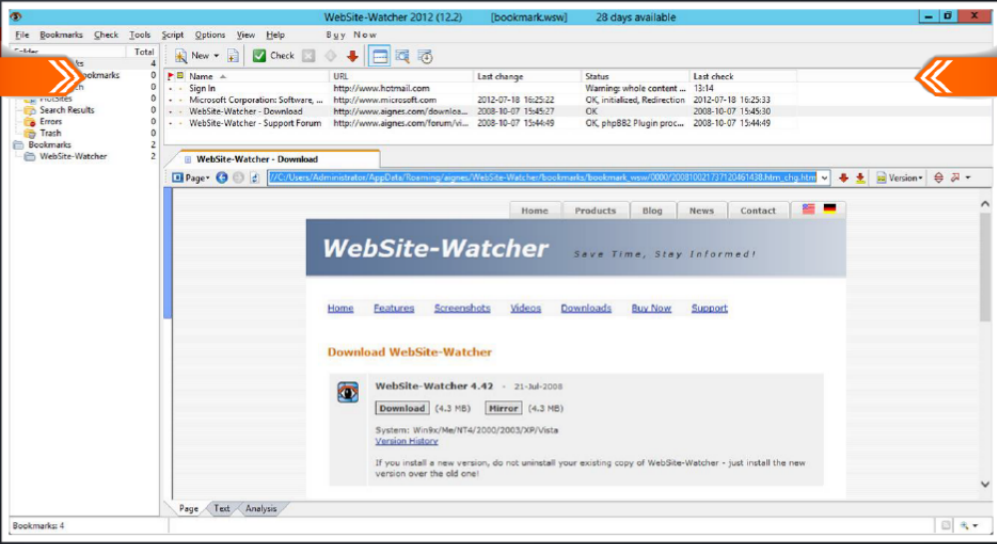


FIGURE 2.22: Internet Archive Wayback Machine screenshot

Monitoring Web Updates Using Website Watcher

Website Watcher automatically checks web pages for updates and changes



The screenshot displays the Website-Watcher 12.2.2 application window. The top menu bar includes File, Bookmarks, Check, Tools, Script, Options, View, and Help. Below the menu is a toolbar with icons for New, Check, and other functions. The main window is divided into two panes. The left pane shows a tree view of monitored websites, including 'Sign-In', 'Microsoft Corporation: Software...', 'Website-Watcher - Download', and 'Website-Watcher - Support Forum'. The right pane shows a table of monitored websites with columns for Name, URL, Last change, Status, and End check. The table lists several websites, including 'http://www.hotmail.com', 'http://www.microsoft.com', 'http://www.aignes.com/downloads...', and 'http://www.aignes.com/forum/vi...'. The bottom pane shows the 'Website-Watcher - Download' page, which includes a 'Download' button and a 'Mirror' button. The page also displays the version number 'Website-Watcher 4.42' and the date '21-Jul-2008'. The status bar at the bottom indicates 'Page: Text Analysis'.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Monitoring Web Updates Using Website Watcher

Source: <http://www.aignes.com>

Website Watcher is used to keep track of websites for updates and automatic changes. When an update or change occurs, Website Watcher automatically detects and saves the last two versions onto your disk, and highlights changes in the text. It is a useful tool for monitoring sites to gain **competitive advantage**.

Benefits:

Frequent manual checking of updates is not required. Website Watcher can automatically detect and notify users of updates:

- It allows you to know what your competitors are doing by scanning your competitors' websites
- The site can keep track of new software versions or driver updates
- It stores images of the modified websites to a **disk**

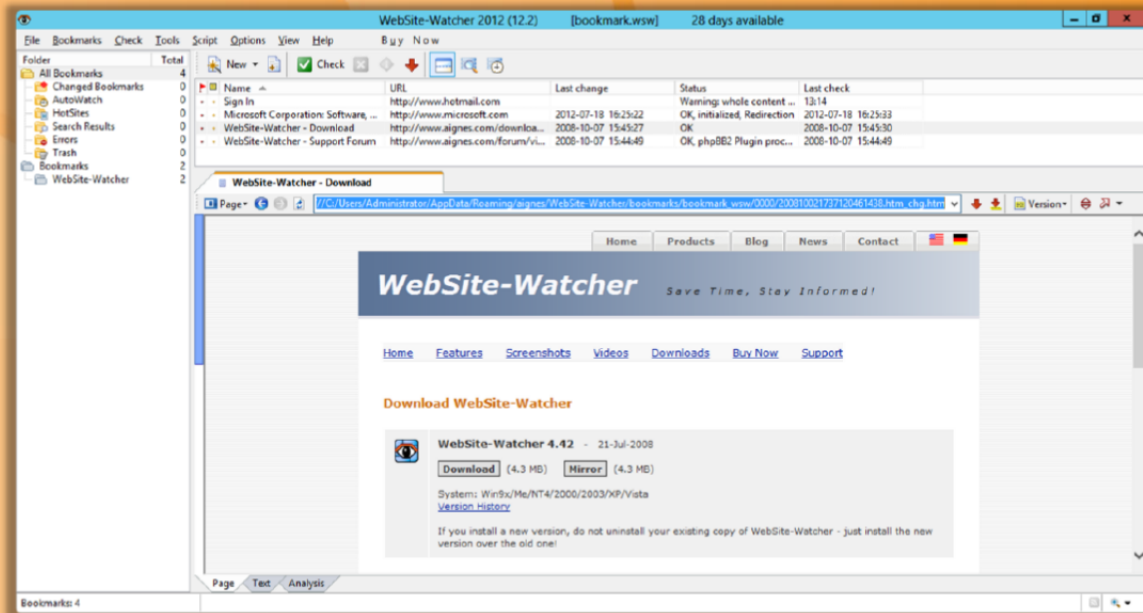


FIGURE 2.23: Website watcher monitoring web updates

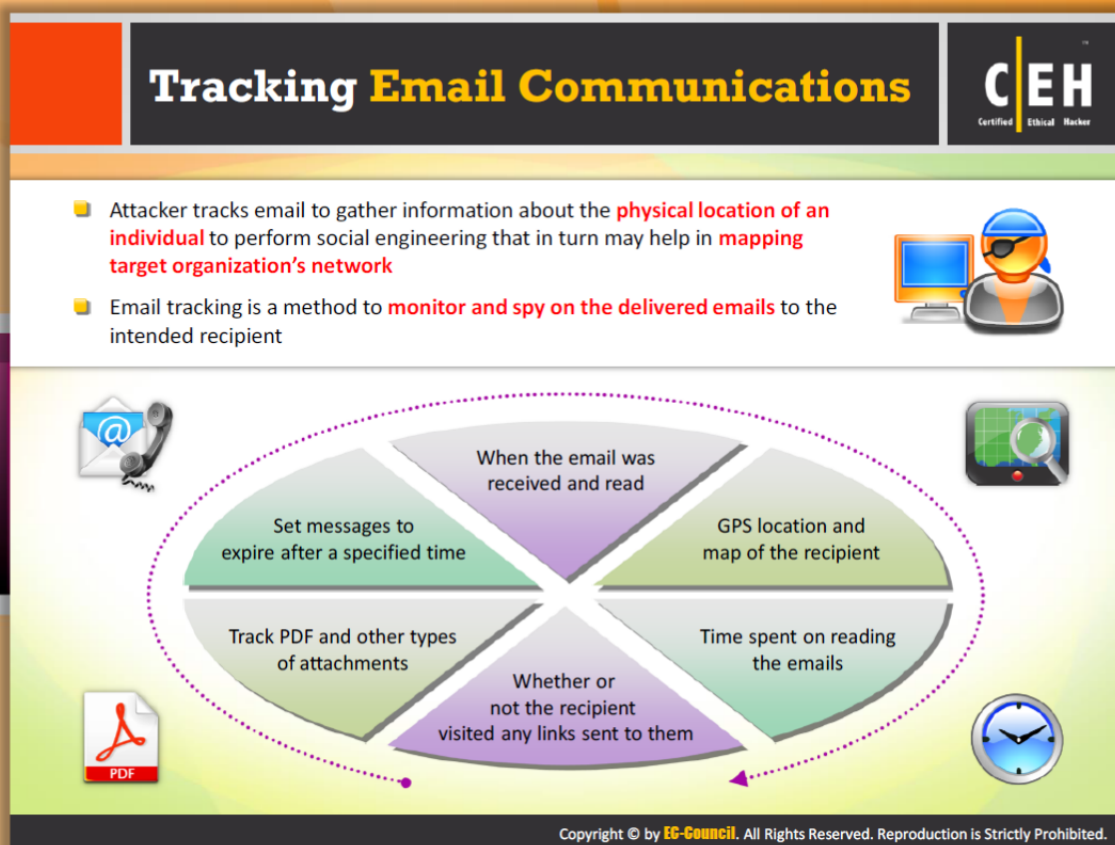


Footprinting Methodology

So far we have discussed Footprinting through search engines and website footprinting, the two initial phases of footprinting methodology. Now we will discuss **email footprinting**.



This section describes how to track email communications, how to collect information from email headers, and email tracking tools.



Tracking Email Communications

Email tracking is a method that helps you to monitor as well as to track the emails of a particular user. This kind of tracking is possible through digitally time stamped records to reveal the time and date a particular email was received or opened by the target. A lot of email **tracking tools** are readily available in the market, using which you can collect information such as IP addresses, mail servers, and service provider from which the mail was sent. Attackers can use this information to build the **hacking strategy**. Examples of email tracking tools include: eMailTrackerPro and Paraben E-mail Examiner.

By using email tracking tools you can gather the following information about the victim:

- **Geolocation:** Estimates and displays the location of the recipient on the map and may even calculate distance from your location.
- **Read duration:** The duration of time spent by the recipient on reading the mail sent by the sender.
- **Proxy detection:** Provides information about the type of server used by the recipient.
- **Links:** Allows you to check whether the links sent to the recipient through email have been checked or not.

- **Operating system:** This reveals information about the type of operating system used by the recipient. The attacker can use this information to launch an attack by finding loopholes in that particular operating system.
- **Forward email:** Whether or not the email sent to you is forwarded to another person can be determined easily by using this tool.

Collecting Information from Email Header

CEH
Certified Ethical Hacker

The screenshot shows an email header with several fields highlighted by callouts:

- The address from which the message was sent:** Points to the `Received: by 10.112.39.167 with SMTP id q7c...` line.
- Sender's IP address:** Points to the `client-ip=10.224.205.137` line.
- Sender's mail server:** Points to the `Authentication-Results: mr.google.com` line.
- Date and time received by the originator's email servers:** Points to the `Received: from mr.google.com ([10.224.205.137])` line.
- Authentication system used by sender's mail server:** Points to the `DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;` line.
- Date and time of message sent:** Points to the `Date: Sat, 2 Jun 2012 09:53:59 +0530` line.
- A unique number assigned by mr.google.com to identify the message:** Points to the `Message-ID: <CAOYWATT1zdDXE3o8D2rhiE4Ber2M...` line.
- Sender's full name:** Points to the `From: Mirza <mirza@mirza@gmail.com>` line.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Collecting Information from Email Headers

An email header is the information that travels with every email. It contains the details of the sender, routing information, date, subject, and recipient. The process of viewing the **email header** varies with different mail programs.

Commonly used email programs:

- SmarterMail Webmail
- Outlook Express 4-6
- Outlook 2000-2003
- Outlook 2007
- Eudora 4.3/5.0
- Entourage
- Netscape Messenger 4.7
- MacMail

The following is a screenshot of a sample email header.


```
Delivered-To: [redacted]@gmail.com
Received: by 10.112.39.167 with SMTP id q7csp489412lbk;
  Fri, 1 Jun 2012 21:24:01 -0700 (PDT)
Return-Path: <[redacted]erma@gmail.com>
Received-SPF: pass (google.com: domain of [redacted]erma@gmail.com designates 10.224.205.137 as permitted
sender) client-ip=10.224.205.137;
Authentication-Results: [redacted]mr.google.com; spf=pass (google.com: domain of [redacted]erma@gmail.com designates
10.224.205.137 as permitted sender) smtp.mail=[redacted]erma@gmail.com; dkim=pass
header.i=[redacted]erma@gmail.com
Received: from mr.google.com ([10.224.205.137])
  by 10.224.205.137 with SMTP id fq9mr8578570qab.39.1338611040773 (num_hops = 1);
  Fri, 01 Jun 2012 21:24:00 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
  d=gmail.com; s=20120113;
  h=mime-version:in-reply-to:references:date:message-id:subject:from:to
  :content-type;
  bh=TGEIPb4ti7gfQG+ghh7OkPjKx+Tt/iAC1PPyWmNgYHc=;
  b=KguZLTLfg2+QZxZKex1NnvRcnD/+P4+Nk5NKSptG7uHXDsFv/hGH46e2P+75MxDR8
  blPK3eJ3Uf/CsaBZWDIT0XLak0AGrP3Bot92MCZFxeUUQ9uWl/xHALSnkeUIEEeKGqOC
  oa9hD59D3oXI8KAC72mkblGzXmV4D1WffCL894RaMBOUoMzRwOWWIib95a1I38cqt1fP
  ZhrWFKh5xSnZxSE73xZFEYzp7yecCeQuYHZNgs1KxcO7xQjeZuw+HWK/vR6xChDjapZ4
  K5ZafYzmIkFX+VdLzqu7YGFzy6oHcuPl6yS/C2fXHVdsuYamMT/yecvHCv08Og7FKt6
  /Kzw==
MIME-Version: 1.0
Received: by 10.224.205.137 with SMTP id fq9mr6704586qab.39.1338611040318;
  Fri, 01 Jun 2012 21:24:00 -0700 (PDT)
Received: by 10.229.230.79 with HTTP; Fri, 1 Jun 2012 21:23:59 -0700 (PDT)
In-Reply-To: <CAOYWATT1zdDXE3o8D2rhiE4Ber2MtV0uhro6r+7Mu7c8ubp8Eg@mail.gmail.com>
References: <CAOYWATT1zdDXE3o8D2rhiE4Ber2MtV0uhro6r+7Mu7c8ubp8Eg@mail.gmail.com>
Date: Sat, 2 Jun 2012 09:53:59 +0530
Message-ID: <CAMSVoXTUqEjnfW8WJdSzQhNnO=EMJcgfgX+mUfjB_tt2sy2dXA@mail.gmail.com>
Subject: ... SOLUTIONS ::
From: [redacted] Mirza <[redacted]erma@gmail.com>
To: [redacted]in@gmail.com,
  [redacted] SOLUTIONS <[redacted]olutions@gmail.com>, [redacted]eed <[redacted]er@yahoo.com>,
```

FIGURE 2.24: Email header screenshot

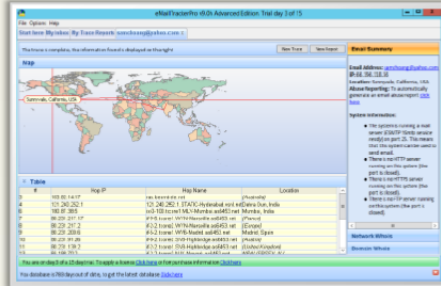
This email header contains the following information:

- Sender's mail server
- Data and time received by the originator's email servers
- Authentication system used by sender's mail server
- Data and time of message sent
- A unique number assigned by mr.google.com to identify the message
- Sender's full name
- Senders IP address
- The address from which the message was sent

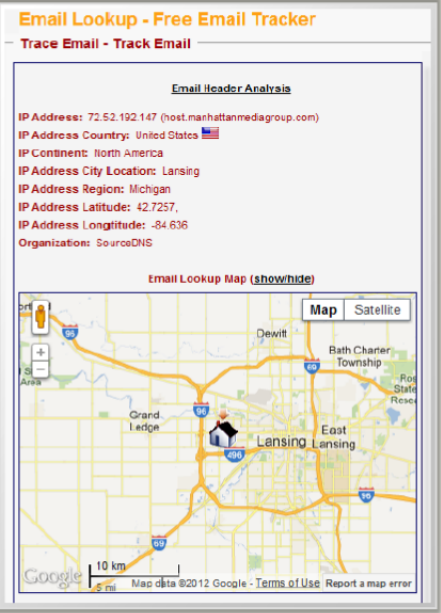
The attacker can trace and collect all of this information by performing a detailed analysis of the complete **email header**.

Email Tracking Tools

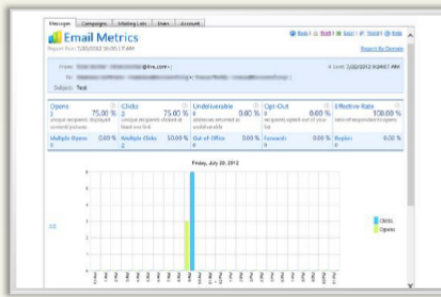




eMailTrackerPro (<http://www.emailtrackerpro.com>)



Email Lookup - Free Email Tracker (<http://www.ipaddresslocation.org>)



PoliteMail (<http://www.politemail.com>)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Email Tracking Tools

Email tracking tools allow you to track an email and extract information such as **sender identity, mail server, sender's IP address**, etc. You can use the extracted information to attack the target organization's systems by sending malicious emails. Numerous email tracking tools are readily available in the market.

The following are a few commonly used email tracking tools:



eMailTrackerPro

Source: <http://www.emailtrackerpro.com>

eMailTrackerPro is an email tracking tool that analyzes email headers and reveals information such as sender's geographical location, IP address, etc. It allows you to review the traces later by saving all past traces.



FIGURE 2.25: eMailTrackerPro showing geographical location of sender



PoliteMail

Source: <http://www.politemail.com>

PoliteMail is an email tracking tool for Outlook. It tracks and provides complete details about who opened your mail and which document has been opened, as well as which links are being clicked and read. It offers mail merging, split testing, and full list management including segmenting. You can compose an email containing **malicious links** and send it to the employees of the target organization and keep track of your email. If the employee clicks on the link, he or she is infected and you will be notified. Thus, you can gain control over the system with the help of this tool.

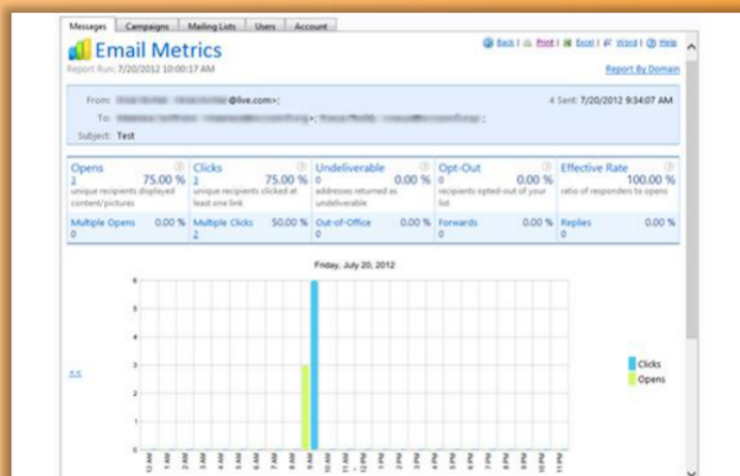


FIGURE 2.26: Politemail screenshot



Email Lookup – Free Email Tracker

Source: <http://www.ipaddresslocation.org>

Email Lookup is an email tracking tool that determines the IP address of the sender by analyzing the **email header**. You can copy and paste the email header into this email tracking tool and start tracing email.

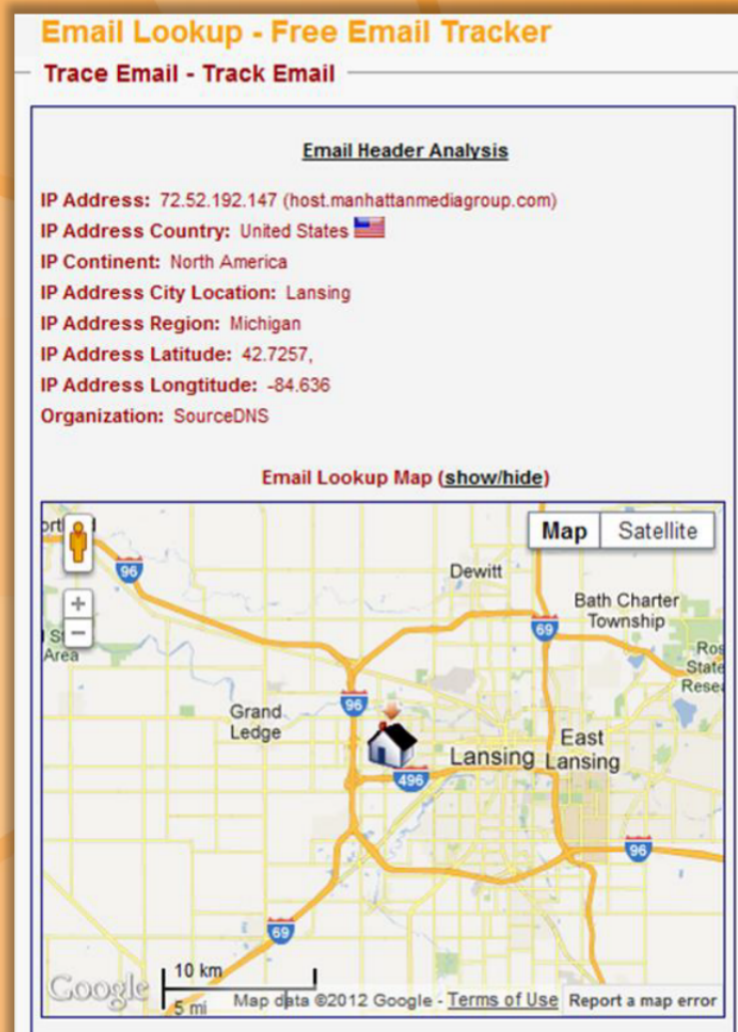


FIGURE 2.27: Email Lookup Screenshot

Email Tracking Tools (Cont'd)



 Read Notify http://www.readnotify.com	 Pointofmail http://www.pointofmail.com
 DidTheyReadIt http://www.didtheyreadit.com	 Super Email Marketing Software http://www.bulk-email-marketing-software.net
 Trace Email http://whatismyipaddress.com	 WhoReadMe http://whoreadme.com
 MSGTAG http://www.msgtag.com	 GetNotify http://www.getnotify.com
 Zendio http://www.zendio.com	 G-Lock Analytics http://glockanalytics.com

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Email Tracking Tools (Cont'd)



Read Notify

Source: <http://www.readnotify.com>

Read Notify provides an email tracking service. It notifies you when a tracked email is opened, re-opened, or forwarded. Read **Notify tracking** reports contain information such as complete delivery details, date and time of opening, geographic location of recipient, visualized map of location, IP address of the recipients, referrer details (i.e., if accessed via web email account etc.), etc.



DidTheyReadIt

Source: <http://www.didtheyreadit.com>

DidTheyReadIt is an email tracking utility. In order to use this utility you need to sign up for an account. Then you need to add ".DidTheyReadIt.com" to the end of the recipient's e-mail address. For example, if you were sending an e-mail to ellen@aol.com, you'd just send it to **ellen@aol.com.DidTheyReadIt.com** instead, and your email would be **tracked. ellen@aol.com** would not see that you added .DidTheyReadIt.com to her email address. This utility tracks every email that you send invisibly, without alerting the recipient. If the user opens your mail, then it

informs you when your mail was opened, how long your email remained open, and the geographic location where your email was viewed.



TraceEmail

Source: <http://whatismyipaddress.com>

The TraceEmail tool attempts to locate the source IP address of an email based on the email headers. You just need to copy and paste the full headers of the target email into the Headers box and then click the Get Source button. It shows the **email header analysis** and results.

This Email header analysis tool does not have the ability to detect forged emails headers. These forged email headers are common in malicious email and spam. This tool assumes all mail servers and email clients in the transmission path are trustworthy.



MSGTAG

Source: <http://www.msgtag.com>

MSGTAG is Windows email tracking software that uses a read receipt technology to tell you when your emails are opened and when your emails are actually read. This software adds a **small track** and trace tag that is unique to each email you need delivery confirmation for. When the email is opened an email tracking code is sent to the MSGTAG email tracking system and an email read confirmation is delivered to you. MSGTAG will notify you when the message is read via an emailed confirmation, a pop-up message, or an **SMS text message**.



Zendio

Source: <http://www.zendio.com>

Zendio, the email tracking software add-in for Outlook, notifies you once your recipient reads the email, so you can follow up, knowing when they read it and if they clicked on any links included in the email.



Pointofmail

Source: <http://www.pointofmail.com>

Pointofmail.com is a proof of receipt and reading service for email. It ensures read receipts, tracks attachments, and lets you modify or delete sent messages. It provides detailed information about the recipient, full history of email reads and forwards, links and attachments tracking, email, and web and SMS text notifications.



Super Email Marketing Software

Source: <http://www.bulk-email-marketing-software.net>

Super Email Marketing Software is a professional and standalone bulk mailer program. It has the ability to send mails to a list of addresses. It supports both text as well as **HTML formatted emails**. All duplicate email addresses are removed automatically by using this application. Each mail is sent individually to the recipient so that the recipient can only see his or her email in the

email header. It saves the email addresses of the successful sent mails as well as the failed mails to a text, CSV, TSV or Microsoft Excel file.



WhoReadMe

Source: <http://whoreadme.com>

WhoReadMe is an email tracking tool. It is completely invisible to recipients. The recipients will have no idea that the emails sent to them are being tracked. The sender is notified every time the recipient opens the mail sent by the sender. It tracks information such as type of operating system and browser used, Active X Controls, CSS version, duration between the mails sent and read time, etc.



GetNotify

Source: <http://www.getnotify.com>

GetNotify is an email tracking tool that sends notifications when the recipient opens and reads the mail. It sends notifications without the knowledge of recipient.



G-Lock Analytics

Source: <http://glockanalytics.com>

G-Lock Analytics is an **email** tracking service. This allows you to know what happens to your emails after they are sent. This tool reports to you how many times the email was printed and forwarded.



Footprinting Methodology

The next phase in footprinting methodology after email footprinting is **competitive intelligence**.

Competitive intelligence is a process that gathers, analyzes, and distributes intelligence about products, customers, competitors, and technologies using the Internet. The information that is gathered can help managers and executives of a company make **strategic decisions**. This section is about competitive intelligence gathering and sources where you can get valuable information.

Competitive Intelligence Gathering



- Competitive intelligence is the process of **identifying, gathering, analyzing, verifying, and using information** about your competitors from resources such as the Internet
- Competitive intelligence is **non-interfering** and **subtle in nature**



Sources of Competitive Intelligence

1 Company websites and employment ads	6 Social engineering employees
2 Search engines, Internet, and online databases	7 Product catalogues and retail outlets
3 Press releases and annual reports	8 Analyst and regulatory reports
4 Trade journals, conferences, and newspaper	9 Customer and vendor interviews
5 Patent and trademarks	10 Agents, distributors, and suppliers

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Competitive Intelligence Gathering

Various tools are readily available in the market for the purpose of competitive intelligence gathering.

Acquisition of information about products, competitors, and technologies of a company using the Internet is defined as competitive intelligence. Competitive intelligence is not just about **analyzing competitors** but also **analyzing their products, customers, suppliers**, etc. that impact the organization. It is non-interfering and subtle in nature compared to the direct intellectual property theft carried out through hacking or industrial espionage. It mainly concentrates on the external business environment. It gathers information ethically and legally instead of gathering it secretly. According to CI professionals, if the intelligence information gathered is not useful, then it is not called intelligence. **Competitive intelligence** is performed for determining:

- What the competitors are doing
- How competitors are positioning their products and services

Sources of Competitive Intelligence:

- Company websites and employment ads
- Search engines, Internet, and online databases

- Press releases and annual reports
- Trade journals, conferences, and newspapers
- Patents and trademarks
- Social engineering employees
- Product catalogs and retail outlets
- Analyst and regulatory reports
- Customer and vendor interviews
- Agents, distributors, and suppliers

Competitive intelligence can be carried out by either employing people to search for the information or by utilizing a commercial database service, which incurs a lower cost than employing personnel to do the same thing.

Competitive Intelligence - When Did this Company Begin? How Did it Develop?

The diagram features a central circle labeled "Company". Surrounding it are four colored circles: "When" (red), "How" (yellow), "Where" (blue), and "Who" (green). Each circle is connected to a question: "When did it begin?" (top), "How did it develop?" (right), "Who leads it?" (bottom), and "Where is it located?" (left). The circles are arranged in a square pattern around the center, with dashed lines connecting them to the central "Company" circle.

Visit These Sites

- 01. EDGAR Database
<http://www.sec.gov/edgar.shtml>
- 02. Hoovers
<http://www.hoovers.com>
- 03. LexisNexis
<http://www.lexisnexis.com>
- 04. Business Wire
<http://www.businesswire.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Competitive Intelligence - When Did this Company Begin? How Did it Develop?

Gathering competitor documents and records helps improve **productivity** and **profitability** and stimulate the growth. It helps determine the answers to the following:

When did it begin?

Through competitive intelligence, the history of a company can be collected, such as when a particular company was established. Sometimes, crucial information that isn't usually available for others can also be collected.

How did it develop?

It is very beneficial to know about how exactly a particular company has developed. What are the various strategies used by the company? Their advertisement policy, customer relationship management, etc. can be learned.

Who leads it?

This information helps a company learn details of the leading person (decision maker) of the company.

Where is it located?

The location of the company and information related to various branches and their operations can be collected through competitive intelligence.

You can use this information gathered through competitive intelligence to build a hacking strategy.

The following are information resource sites that help users **gain competitive intelligence**.



EDGAR

Source: <http://www.sec.gov/edgar.shtml>

All companies, foreign and domestic, are required to file registration statements, periodic reports, and other forms electronically through EDGAR. Anyone can view the **EDGAR database** freely through the Internet (web or FTP). All the documents that are filed with the commission by public companies may not be available on EDGAR.



Hoovers

Source: <http://www.hoovers.com>

Hoovers is a business research company that provides complete details about companies and industries all over the world. Hoovers provides patented business-related information through Internet, data feeds, wireless devices, and co-branding agreements with other online services. It gives complete information about the organizations, industries, and people that drive the economy and also provide the tools for connecting to the right people, in order for getting business done.



LexisNexis

Source: <http://www.lexisnexis.com>

LexisNexis is a global provider of content-enabled workflow solutions designed specifically for **professionals in the legal, risk management, corporate, government, law enforcement, accounting, and academic markets**. It maintains an electronic database through which you can get legal and public-records related information. Documents and records of legal, news, and business sources are made accessible to customers.



Business Wire

Source: <http://www.businesswire.com>

Business Wire is a company that focuses on press release distribution and regulatory disclosure. Full text news releases, photos, and other multimedia content from thousands of companies and organizations are distributed by this company across the globe to journalists, news media, financial markets, investors, information website, databases, and general audiences. This company has its own patented electronic network through which it releases its news.

Competitive Intelligence - What Are the Company's Plans?





Competitive Intelligence Sites

✓ Market Watch (http://www.marketwatch.com)	MarketWatch
✓ The Wall Street Transcript (http://www.twst.com)	twst.com
✓ Lipper Marketplace (http://www.lippermarketplace.com)	LIPPER MARKETPLACE
✓ Euromonitor (http://www.euromonitor.com)	EUROMONITOR INTERNATIONAL
✓ Fagan Finder (http://www.faganfinder.com)	Fagan Finder
✓ SEC Info (http://www.secinfo.com)	SEC Info
✓ The Search Monitor (http://www.thesearchmonitor.com)	THE SEARCH MONITOR

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Competitive Intelligence - What Are the Company's Plans?

The following are a few more examples of websites that are useful to gather valuable information about various companies and their plans through **competitive intelligence**:



MarketWatch

Source: <http://www.marketwatch.com>

MarketWatch tracks the pulse of markets. The site provides business news, personal finance information, real-time commentary, and investment tools and data, with dedicated journalists generating hundreds of headlines, stories, videos, and market briefs a day.



The Wall Street Transcript

Source: <http://www.twst.com>

The Wall Street Transcript is a website as well as paid subscription publication that publishes industry reports. It expresses the views of money managers and equity analysts of different industry sectors. Interviews with CEOs of companies are published.



Lipper Marketplace

Source: <http://www.lippermarketplace.com>

Lipper Marketplace offers web-based solutions that are helpful for identifying the market of a company. Marketplace helps in qualifying prospects and provides the competitive intelligence needed for transforming these prospects into clients. Its solutions allow users to identify net flows and track institutional trends.



Euromonitor

Source: <http://www.euromonitor.com>

Euromonitor provides strategy research for consumer markets. It publishes reports on industries, consumers, and demographics. It provides market research and surveys focused on your organization's needs.



Fagan Finder

Source: <http://www.faganfinder.com>

Fagan Finder is a collection of internet tools. It is a directory of blog sites, news sites, search engines, photo sharing sites, science and education sites, etc. Specialized tools such as Translation Wizard and URL info are available for finding information about various actions with a web page.



SEC Info

Source: <http://www.secinfo.com>

SEC Info offers the U.S. Securities and **Exchange Commission (SEC) EDGAR** database service on the web, with billions of links added to the SEC documents. It allows you to search by Name, Industry, and Business, SIC Code, Area Code, Accession Number, File Number, CIK, Topic, ZIP Code, etc.



The Search Monitor

Source: <http://www.thesearchmonitor.com>

The Search Monitor provides real-time competitive intelligence to monitor a number of things. It allows you to monitor market share, page rank, ad copy, landing pages, and the budget of your competitors. With the **trademark monitor**, you can monitor the buzz about yours as well as your competitor's brand and with the affiliate monitor; you can watch monitor ad and landing page copy.



Competitive Intelligence - What Expert Opinions Say About the Company



Copernic Tracker

Source: <http://www.copernic.com>

Copernic is website tracking software. It monitors a competitor's website continuously and acknowledges you content changes via an email, if any. The updated pages as well as the changes made in the site are highlighted for your convenience. You can even watch for specific keywords, to see the changes made on your **competitor's sites**.



SEMRush

Source: <http://www.semrush.com>

SEMRush is a competitive keyword research tool. For any site, you can get a list of Google keywords and AdWords, as well as a competitors list in the organic and paid Google search results. Necessary means for gaining in-depth knowledge about what competitors are advertising and their budget allocation to specific Internet marketing tactics are provided by SEMRush



Jobitorial

Source: <http://www.jobitorial.com>

Jobitorial provides anonymous employee reviews posted for jobs at thousands of companies and allows you to review a company.



AttentionMeter

Source: <http://www.attentionmeter.com>

AttentionMeter is a tool used for comparing any website you want (traffic) by using Alexa, Compete, and Quancast. It gives you a snapshot of traffic data as well as graphs from Alexa, Compete, and QuantCast.



ABI/INFORM Global

Source: <http://www.proquest.com>

ABI/INFORM Global is a business database. ABI/INFORM Global offers the latest business and financial information for researchers at all levels. With ABI/INFORM Global, users can determine business conditions, management techniques, business trends, management practice and theory, corporate strategy and tactics, and the competitive landscape.



Compete PRO

Source: <http://www.compete.com>

Compete PRO provides an online **competitive intelligence service**. It combines all the site, search, and referral analytics in a single product.



Footprinting Methodology



Footprinting using Google

Though Google is a search engine, the process of footprinting using Google is not similar to the process of footprinting through search engines. Footprinting using Google deals with gathering information by Google hacking. Google hacking is a hacking technique to **locate specific strings** of text within search results using an advanced operator in Google search engine. Google will filter for excessive use of advanced search operators and will drop the requests with the help of an Intrusion Prevention System



Footprinting using Google Hacking Techniques

Google hacking refers to the art of creating complex search engine queries. If you can construct proper queries, you can retrieve valuable data about a target company from the Google search results. Through Google hacking, an attacker tries to find websites that are vulnerable to numerous exploits and vulnerabilities. This can be accomplished with the help of Google hacking database (GHDB), a database of queries to identify sensitive data. Google operators help in finding required text and avoiding irrelevant data. Using advanced Google operators, attackers locate specific strings of text such as specific versions of vulnerable web applications.

Some of the popular Google operators include:

- **.Site:** The .Site operator in Google helps to find only pages that belong to a specific URL.
- **allinurl:** This operator finds the required pages or websites by restricting the results containing all query terms.
- **Inurl:** This will restrict the results to only websites or pages that contain the query terms that you have specified in the URL of the website.
- **allintitle:** It restricts results to only web pages that contain all the query terms that you have specified.

- **intitle:** It restricts results to only the web pages that contain the query term that you have specified. It will show only websites that mention the query term that you have used.
- **Inanchor:** It restricts results to pages containing the query term that you have specified in the anchor text on links to the page.
- **Allinanchor:** It restricts results to pages containing all query terms you specify in the anchor text on links to the page.



What Can a Hacker Do with Google Hacking?

If the target website is vulnerable to Google hacking, then the attacker can find the following with the help of queries in Google hacking database:

- Error messages that contain sensitive information
- Files containing passwords
- Sensitive directories
- Pages containing logon portals
- Pages containing network or vulnerability data
- Advisories and server vulnerabilities

Google Advance Search Operators



Google supports several advanced operators that help in **modifying the search**

[cache:]	 Displays the web pages stored in the Google cache	
[link:]	 Lists web pages that have links to the specified web page	
[related:]	 Lists web pages that are similar to a specified web page	
[info:]	 Presents some information that Google has about a particular web page	
[site:]	 Restricts the results to those websites in the given domain	
[allintitle:]	 Restricts the results to those websites with all of the search keywords in the title	
[intitle:]	 Restricts the results to documents containing the search keyword in the title	
[allinurl:]	 Restricts the results to those with all of the search keywords in the URL	
[inurl:]	 Restricts the results to documents containing the search keyword in the URL	

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Google Advance Search Operators

Source: <http://www.googleguide.com>

Cache: The CACHE query displays Google's cached version of a web page, instead of the current version of the page.

Example:

cache: www.eff.org will show Google's cached version of the Electronic Frontier Foundation home page.

Note: Do not put a space between cache: and the URL (web address).

link: Link lists web pages that have links to the specified web page. For example, to find pages that point to Google Guide's home page, enter:

link: www.googleguide.com

Note: According to Google's documentation, "you cannot combine a link: search with a regular keyword search."

Also note that when you combine link: with another advanced operator, Google may not return all the pages that match. The following queries should return lots of results, as you can see if you remove the -site: term in each of these queries.

related: If you start your query with "related:", then Google displays websites similar to the site mentioned in the search query.

Example: related:www.microsoft.com will provide the Google search engine results page with websites similar to microsoft.com.

info: Info will present some information the corresponding web page.

For instance, info:gothotel.com will show information about the national hotel directory GotHotel.com home page.

Note: There must be no space between the info: and the web page URL.

This functionality can also be obtained by typing the web page URL directly into a Google search box.

site: If you include site: in your query, Google will restrict your search results to the site or domain you specify.

For example, admissions site:www.lse.ac.uk will show admissions information from London School of Economics' site and [peace site:gov] will find pages about peace within the .gov domain. You can specify a domain with or without a period, e.g., either as .gov or gov.

Note: Do not include a space between the "site:" and the domain.

allintitle: If you start your query with allintitle:, Google restricts results to those containing all the query terms you specify in the title.

For example, allintitle: detect plagiarism will return only documents that contain the words "detect" and "plagiarism" in the title. This functionality can also be obtained through the Advanced Web Search page, under Occurrences.

intitle: The query intitle: term restricts results to documents containing term in the title. For instance, flu shot intitle:help will return documents that mention the word "help" in their titles, and mention the words "flu" and "shot" anywhere in the document (title or not).

Note: There must be no space between the intitle: and the following word.

allinurl: If you start your query with allinurl:, Google restricts results to those containing all the query terms you specify in the URL.

For example, allinurl: google faq will return only documents that contain the words "google" and "faq" in the URL, such as "www.google.com/help/faq.html." This functionality can also be obtained through the Advanced Web Search page, under Occurrences.

In URLs, words are often run together. They need not be run together when you're using allinurl.

inurl: If you include inurl: in your query, Google will restrict the results to documents containing that word in the URL.

For instance, inurl:print site:www.googleguide.com searches for pages on Google Guide in which the URL contains the word "print." It finds PDF files that are in the directory or folder named "print" on the Google Guide website. The query [inurl:healthy eating] will return

documents that mention the words “healthy” in their URL, and mention the word “eating” anywhere in the document.

Note: There must be no space between the inurl: and the following word.

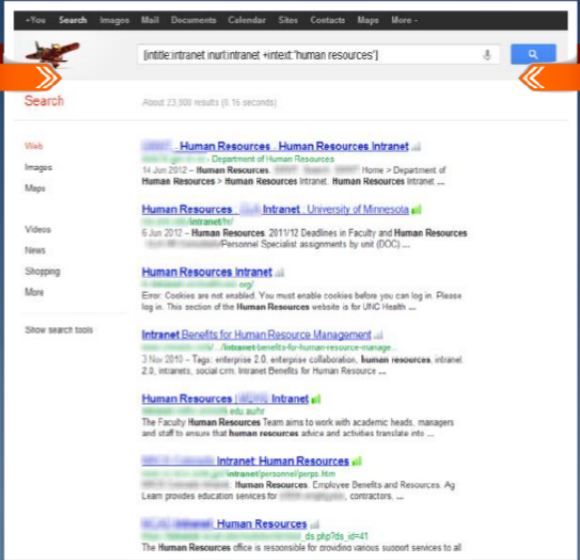
Finding Resources Using Google Advance Operator

CEH
Certified Ethical Hacker

[intitle:intranet inurl:intranet +intext:"human resources"]:

The above combination of the Google advanced search operators allows you to access a target company's private network and collect **sensitive information** such as **employee listings**, **key contact details**, etc. that can be incredibly useful for any social engineering endeavor





Search About 23,500 results (0.16 seconds)

Web **Human Resources - Human Resources Intranet** ...
Images **Department of Human Resources** ...
Maps **Human Resources** ...
Videos **Human Resources Intranet** ...
News **Human Resources Intranet** ...
Shopping **Human Resources Intranet** ...
More **Human Resources Intranet** ...

Show search tools

Intranet Benefits for Human Resource Management ...
Human Resources Intranet ...
Intranet Human Resources ...
Human Resources Intranet ...

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Finding Resources using Google Advance Operator

By using the Google Advance Operator syntax `[intitle:intranet inurl:intranet +intext:"human resources"]`: the attacker can find private information of a target company as well as sensitive information about the employees of that particular company. The information gathered by the attackers can be used to perform social engineering attacks. Google will filter for excessive use of advanced search operators and will drop the requests with the help of an Intrusion Prevention System.

The following screenshot shows a Google search engine results page displaying the results of the previously mentioned query:

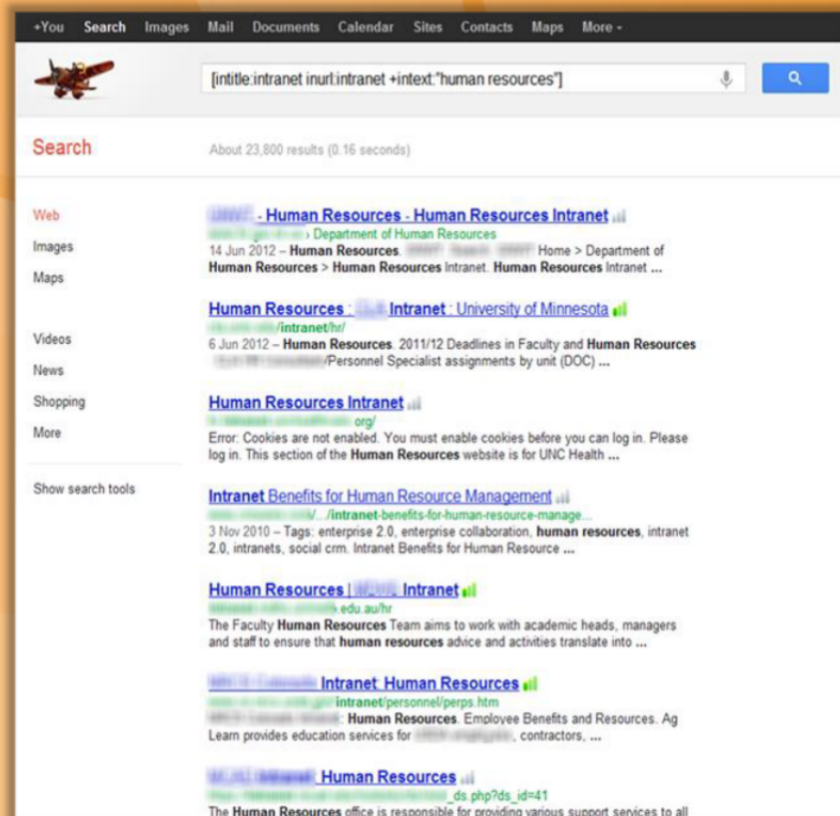
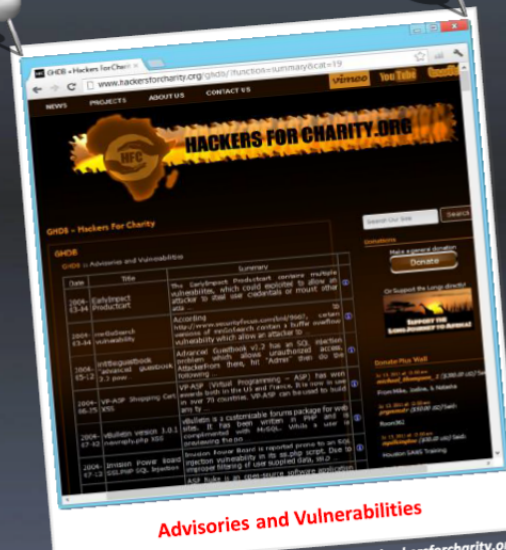


FIGURE 2.28: Search engine showing results for given Google Advance Operator syntax

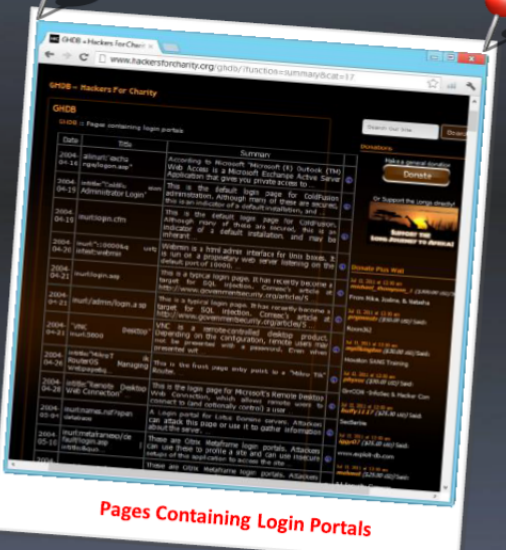
Google Hacking Tool: Google Hacking Database (GHDB)





Advisories and Vulnerabilities

<http://www.hackersforcharity.org>



Pages Containing Login Portals

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Google Hacking Tool: Google Hacking Database (GHDB)

Source: <http://www.hackersforcharity.org>

The Google Hacking database (GHDB) is a database of queries that identify sensitive data. GHDB is an **HTML/JavaScript wrapper application** that uses advanced JavaScript techniques to scrape information from Johnny's Google Hacking Database without the need for hosted server-side scripts. The Google Hacking Database exposes known issues with software that run websites. There are some bugs that expose information that might not warrant public reading.

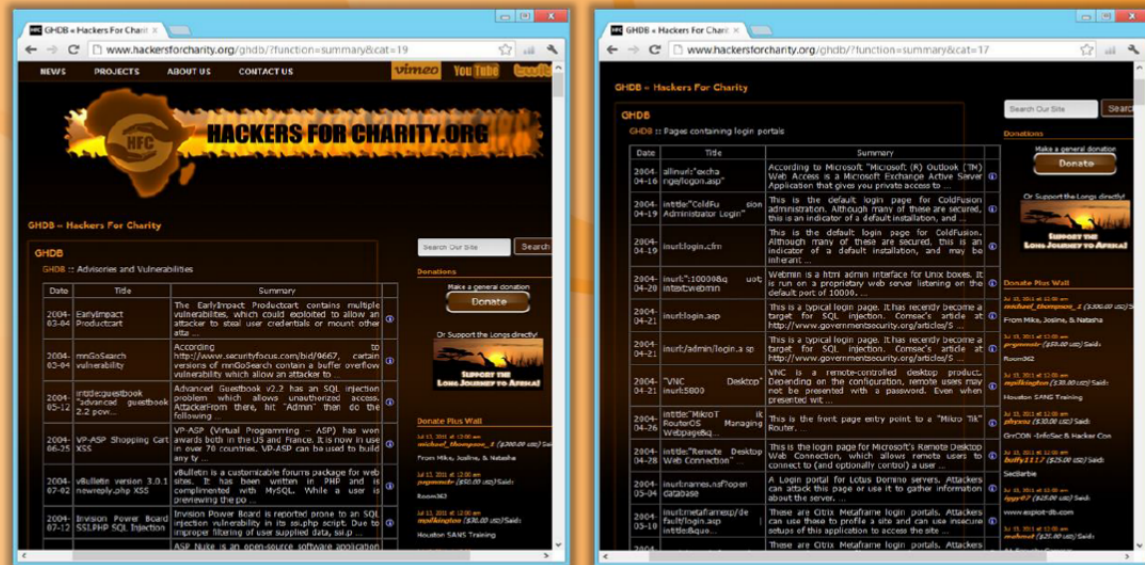


FIGURE 2.29: Screenshots showing Advisories and Vulnerabilities & pages containing login portals

Google Hacking Tools



 MetaGoofil http://www.edge-security.com	 Google Hack Honeypot http://ghh.sourceforge.net
 Goolink Scanner http://www.ghacks.net	 GMapCatcher http://code.google.com
 SiteDigger http://www.mcafee.com	 SearchDiggity http://www.stachliu.com
 Google Hacks http://code.google.com	 Google HACK DB http://www.secpoint.com
 BiLe Suite http://www.sensepost.com	 Gooscan http://www.darknet.org.uk

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Google Hacking Tools

Besides the **Google Hacking Database** (GHDB) tool featured previously, there are some other tools that can help you with Google hacking. There are a few more Google hacking tools mentioned as follows. Using these tools, attackers can gather advisories and server vulnerabilities, error message information that may reveal attack paths, sensitive files, directories, logon portals, etc.



Metagoofil

Source: <http://www.edge-security.com>

Metagoofil is an **information-gathering tool** designed for extracting metadata of public documents (pdf, doc, xls, ppt, docx, pptx, xlsx) belonging to a target company.

Metagoofil performs a search in Google to identify and download the documents to a local disk and then extracts the metadata with different libraries such as Hachoir, PdfMiner?, and others. With the results, it generates a report with usernames, software versions, and servers or machine names that may help **penetration testers** in the information gathering phase.



Goolink Scanner

Source: <http://www.ghacks.net>

The Goolink Scanner **removes the cache** from your searches, and collects and displays only vulnerable site's links. Thus, it allows you to find vulnerable sites wide open to Google and googlebots.



SiteDigger

Source: <http://www.mcafee.com>

SiteDigger searches Google's cache to look for vulnerabilities, errors, configuration issues, proprietary information, and **interesting security nuggets** on websites.



Google Hacks

Source: <http://code.google.com>

Google Hacks is a compilation of carefully crafted Google searches that **expose novel functionality** from Google's search and map services. It allows you to view a timeline of your search results, view a map, search for music, search for books, and perform many other specific kinds of searches.



BiLE Suite

Source: <http://www.sensepost.com>

BiLE stands for **Bi-directional** Link Extractor. The BiLE suite includes a couple of Perl scripts used in enumeration processes. Each Perl script has its own functionality. BiLE.pl is the first tool or Perl script in the collection. BiLE leans on Google and HTTrack to automate the collections to and from the target site, and then applies a simple **statistical weighing algorithm** to deduce which websites have the strongest relationships with the target site.



Google Hack Honeypot

Source: <http://ghh.sourceforge.net>

Google Hack Honeypot is the reaction to a new type of **malicious web traffic**: search engine hackers. It is designed to provide reconnaissance against attackers that use search engines as a hacking tool against your resources. GHH implements the honeypot theory to provide additional security to your web presence.



GMapCatcher

Source: <http://code.google.com>

GMapCatcher is an **offline maps viewer**. It displays maps from many providers such as: CloudMade, OpenStreetMap, Yahoo Maps, Bing Maps, Nokia Maps, and SkyVector. maps.py is a GUI program used to browse Google map. With the offline toggle button unchecked, it can download Google map tiles automatically. Once the file downloads, it resides on your hard disk. Thus, you don't need to download it again.



SearchDiggity

Source: <http://www.stachliu.com>

SearchDiggity is the primary attack tool of the **Google Hacking Diggity Project**. It is Stach & Liu's MS Windows GUI application that serves as a front-end to the most recent versions of Diggity tools such as GoogleDiggity, BingDiggity, Bing LinkFromDomainDiggity, CodeSearchDiggity, DLPDiggity, MalwareDiggity, PortScanDiggity, SHODANDiggity, BingBinaryMalwareSearch, and NotInMyBackYard Diggity.



Google HACK DB

Source: <http://www.secpoint.com>

The attacker can also use the SecPoint Google HACK DB tool to determine sensitive information from the target site. This tool helps an attacker to extract files containing passwords, database files, clear text files, customer database files, etc.



Gooscan

Source: <http://www.darknet.org.uk>

Gooscan is a tool that automates queries against **Google search appliances**. These queries are designed to find potential vulnerabilities on web pages.



Footprinting Methodology

Gathering **network-related** information such as whois information of the target organization is very important when hacking a system. So, now we will discuss whois footprinting.

Whois footprinting focuses on how to perform a whois lookup, analyzing the whois lookup results, and the tools to gather whois information.

WHOIS Lookup



WHOIS databases are maintained by **Regional Internet Registries** and contain the **personal information of domain owners**



WHOIS query returns:

- Domain name details
- Contact details of domain owner
- Domain name servers
- NetRange
- When a domain has been created
- Expiry records
- Records last updated



Information obtained from WHOIS database assists an attacker to:

- Create detailed map of organizational network
- Gather personal information that assists to perform social engineering
- Gather other internal network details, etc.



Regional Internet Registries (RIRs)



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



WHOIS Lookup

WHOIS is a query and response protocol used for **querying databases** that stores the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system. WHOIS databases are maintained by Regional Internet Registries and contain the personal information of domain owners. They maintain a record called a **LOOKUP table** that contains all the information associated with a particular network, domain, and host. Anyone can connect and query to this server to get information about particular networks, domains, and hosts.

An attacker can send a query to the appropriate **WHOIS** server to obtain the information about the target domain name, contact details of its owner, expiry date, creation date, etc. The WHOIS server will respond to the query with respective information. Then, the attacker can use this information to create a map of the organization network, trick domain owners with social engineering once he or she gets contact details, and then get **internal details** of the network.

WHOIS Lookup Result Analysis



Whois Record | Site Profile | Registration | Server Data | My Whois

Registrant:
Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond WA 98052
US
domains@microsoft.com +1.4258828080 Fax: +1.4259367329

Domain Name: microsoft.com

Registrar Name: Markmonitor.com
Registrar Whois: whois.markmonitor.com
Registrar Homepage: http://www.markmonitor.com

Administrative Contact:
Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond WA 98052
US
domains@microsoft.com +1.4258828080 Fax: +1.4259367329

Technical Contact, Zone Contact:
MSN Hostmaster
Microsoft Corporation
One Microsoft Way
Redmond WA 98052
US
manhst@microsoft.com +1.4258828080 Fax: +1.4259367329

Created on.....: 1991-05-01.
Expires on.....: 2021-05-02.
Record last updated on.: 2011-05-16.

Domain servers in listed order:
ns5.msft.net
ns4.msft.net
ns1.msft.net
ns3.msft.net
ns2.msft.net

<http://whois.domaintools.com>

Domain Dossier Investigate domains and IP addresses

domain or IP address:

☒ domain whois record ☒ DNS records ☐ traceroute
☒ network whois record ☐ service scan go

user: anonymous [00:00:00:30]
balance: 47 units
[log in / account info](#) [Central Ops.net](#)

Address lookup
canonical name: juggyboy.com.
aliases:
addresses: www.centralops.net

Domain Whois record
Queried whois.internic.net with "dom juggyboy.com"...

Domain Name: JUGGYBOY.COM
Registrar: NETWORK SOLUTIONS, LLC
Whois Server: whois.networksolutions.com
Referral URL: http://www.networksolutions.com/en_US/
Name Server: NS19.WORLWID.COM
Name Server: NS20.WORLWID.COM
Status: clientTransferProhibited
Updated Date: 03-feb-2009
Creation Date: 16-jul-2002
Expiration Date: 16-jul-2014

>>> Last update of whois database: Thu, 19 Jul 2012 07:49:56 UTC <<<
Queried whois.networksolutions.com with "juggyboy.com"...

Registrant:
Name: JESSIE
ATTN: JESSIE@JUGGYBOY.COM
care of Network Solutions
90 Box 459
Greene, WA. US 98222

<http://centralops.net/co>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



WHOIS Lookup Result Analysis

A whois lookup can be performed using Whois services such as <http://whois.domaintools.com> or <http://centralops.net/co>. Here you can see the result analysis of a Whois lookup obtained with the two mentioned Whois services. Both these services allow you to perform whois lookup by entering the target's domain or IP address. The domaintools.com service provides whois information such as registrant information, email, administrative contact information, created and expiry date, a list of domain servers, etc. The Domain Dossier available at <http://centralops.net/co/> gives the address lookup, domain Whois record, network whois record, and **DNS records information**.

The figure consists of two side-by-side screenshots of web-based Whois services.

Left Screenshot (http://whois.domaintools.com): This is a 'Whois Record' for the domain `microsoft.com`. It displays detailed information about the registrant (Microsoft Corporation), administrative contact, and technical contact. It also shows the domain's creation and expiration dates, and a list of domain servers.

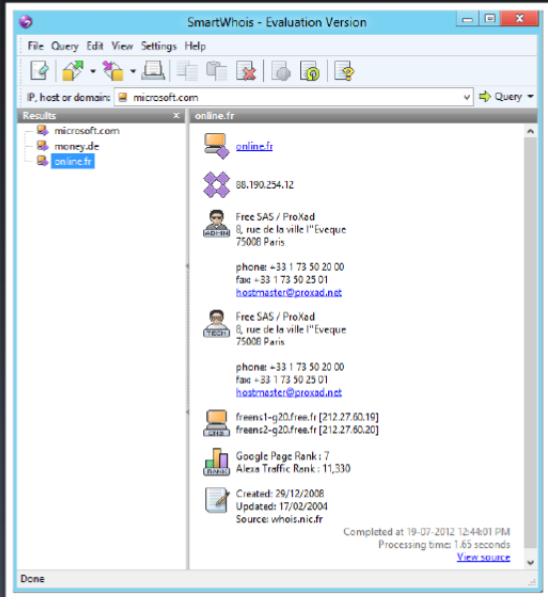
Right Screenshot (http://centralops.net/co): This is a 'Domain Dossier' for the domain `juggyboy.com`. It includes a search bar, checkboxes for various lookup options (domain whois, DNS records, traceroute, network whois, service scan), and a 'Go' button. Below the search bar, it shows the user's anonymous balance and login options. The 'Address lookup' section displays the canonical name, aliases, and addresses for `juggyboy.com`. The 'Domain Whois record' section shows the queried whois.internic.net record for `juggyboy.com`, including domain name, registrar, whois server, referral URL, name servers, status, and creation/expiration dates.

FIGURE 2.30: Whois services screenshots

WHOIS Lookup Tool: SmartWhois



- SmartWhois is a useful network information utility that allows you to look up all the available information about an **IP address**, **hostname**, or **domain**
- It also provides information about **country**, **state or province**, **city**, name of the network provider, administrator, and technical support contact information



SmartWhois - Evaluation Version

File Query Edit View Settings Help

IP, host or domain: microsoft.com

Results

- microsoft.com
- money.de
- online.fr

online.fr

06.190.254.12

Free SAS / Proxad
0, rue de la ville l'Eveque
75008 Paris

phone: +33 1 73 50 20 00
fax: +33 1 73 50 25 01
hostmaster@proxad.net

Free SAS / Proxad
0, rue de la ville l'Eveque
75008 Paris

phone: +33 1 73 50 20 00
fax: +33 1 73 50 25 01
hostmaster@proxad.net

freem1-q20.free.fr [212.27.60.16]
freem2-q20.free.fr [212.27.60.20]

Google Page Rank: 7
Alexa Traffic Rank: 11,330

Created: 26/12/2008
Updated: 17/02/2004
Source: whois.nic.fr

Completed at 19-07-2012 12:48:01 PM
Processing time: 1.65 seconds
[View source](http://www.tamos.com)

Done

<http://www.tamos.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



WHOIS Lookup Tool: SmartWhois

Source: <http://www.tamos.com>

SmartWhois is a useful **network information** utility that allows you to look up all the available information about an IP address, hostname, or domain, including country, state or province, city, name of the network provider, administrator, and technical support contact information. It also assists you in finding the owner of the domain, the owner's contact information, the owner of the **IP address block**, registered date of the domain, etc.

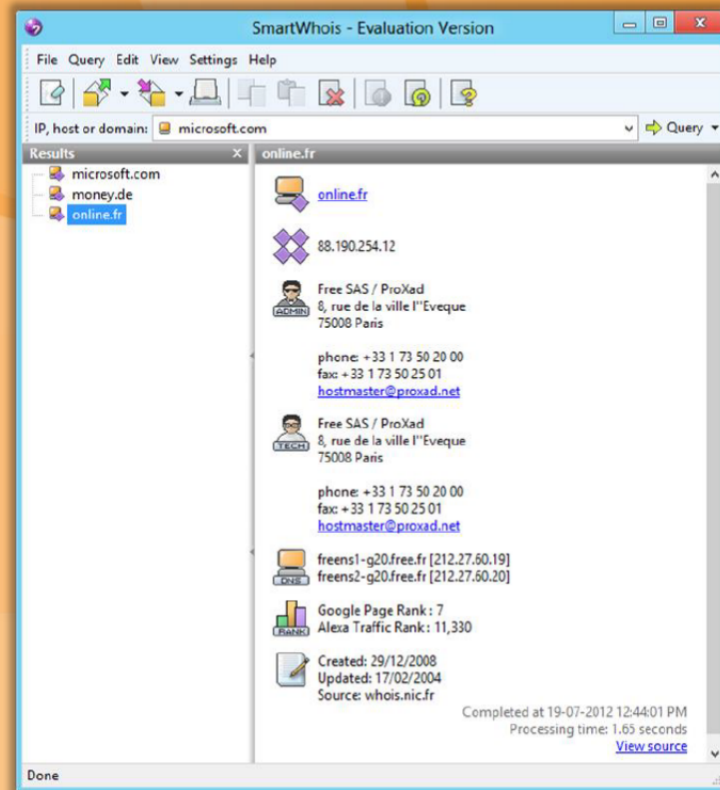


FIGURE 2.31: SmartWhois screenshot

WHOIS Lookup Online Tools



 SmartWhois http://smartwhois.com	 Whois http://tools.whois.net
 Better Whois http://www.betterwhois.com	 DNSstuff http://www.dnsstuff.com
 Whois Source http://www.whois.sc	 Network Solutions Whois http://www.networksolutions.com
 Web Wiz http://www.webwiz.co.uk/domain-tools/whois-lookup.htm	 WebToolHub http://www.webtoolhub.com/tn561381-whois-lookup.aspx
 Network-Tools.com http://network-tools.com	 Ultra Tools https://www.ultratools.com/whois/home

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



WHOIS Lookup Tools

Similar to SmartWhois, there are numerous tools available in the market to retrieve Whois information. A few are mentioned as follows:



CountryWhois

Source: <http://www.tamos.com>

CountryWhois is a utility for identifying the **geographic location of an IP address**. CountryWhois can be used to analyze server logs, check email address headers, identify online credit card fraud, or in any other instance where you need to quickly and accurately determine the country of origin by IP address.



LanWhoIs

Source: <http://lantricks.com>

LanWhoIs provides information about **domains** and **addresses** on the Internet. This program helps you determine who, where, and when the domain or site you are interested in was registered, and the information about those who support it now. This tool allows you to save your search result in the form of an archive to view it later. You can print and save the search result in HTML format.



Batch IP Converter

Source: <http://www.networkmost.com>

Batch IP Converter is a network tool to work with IP addresses. It combines Domain-to-IP Converter, Batch Ping, Tracert, Whois, Website Scanner, and Connection Monitor into a single interface as well as an **IP-to-Country Converter**. It allows you to look up the IP address for a single or list of domain names and vice versa.



CallerIP

Source: <http://www.callerippro.com>

CallerIP is basically IP and port monitoring software that displays the incoming and outgoing connection made to your computer. It also allows you to find the origin of all connecting IP addresses on the world map. The Whois reporting feature provides key information such as who an IP is registered to along with **contact email addresses** and **phone numbers**.



WhoIs Lookup Multiple Addresses

Source: <http://www.sobolsoft.com>

This software offers a solution for users who want to **look up ownership details** for one or more IP addresses. Users can simply enter **IP addresses** or load them from a file. There are three options for lookup sites: whois.domaintools.com, whois-search.com, and whois.arin.net. The user can set a delay period between lookups, to avoid lockouts from these websites. The resulting list shows the IP addresses and details of each. It also allows you to save results to a text file.



WhoIs Analyzer Pro

Source: <http://www.whoisanalyzer.com>

This tool allows you to access information about a **registered domain worldwide**; you can view the domain owner name, domain name, and contact details of domain owner. It also helps in finding the location of a specific domain. You can also submit multiple queries with this tool simultaneously. This tool gives you the ability to print or save the result of the query in **HTML format**.



HotWhois

Source: <http://www.tialsoft.com>

HotWhois is an IP tracking tool that can **reveal valuable information**, such as country, state, city, address, contact phone numbers, and email addresses of an IP provider. The query mechanism resorts to a variety of Regional Internet Registries, to obtain IP Whois information about IP address. With HotWhois you can make whois queries even if the registrar, supporting a particular domain, doesn't have the **whois server itself**.



Whois 2010 Pro

Source: <http://lapshins.com>

Whois 2010 PRO is **network information software** that allows you to look up all the available information about a domain name, including country, state or province, city, administrator, and technical support contact information.



ActiveWhois

Source: <http://www.johnru.com>

ActiveWhois is a network tool to find information about the owners of IP addresses or Internet domains. You can determine the country, personal and postal addresses of the owner, and/or users of IP addresses and domains.



WhoisThisDomain

Source: <http://www.nirsoft.net>

WhoisThisDomain is a domain registration lookup utility that allows you to get information about a registered domain. It automatically connects to the right WHOIS server and retrieves the WHOIS record of the domain. It supports both generic domains and country code domains.

WHOIS Lookup Online Tools



 SmartWhois http://smartwhois.com	 Whois http://tools.whois.net
 Better Whois http://www.betterwhois.com	 DNSstuff http://www.dnsstuff.com
 Whois Source http://www.whois.sc	 Network Solutions Whois http://www.networksolutions.com
 Web Wiz http://www.webwiz.co.uk/domain-tools/whois-lookup.htm	 WebToolHub http://www.webtoolhub.com/tn561381-whois-lookup.aspx
 Network-Tools.com http://network-tools.com	 Ultra Tools https://www.ultratools.com/whois/home

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



WHOIS Lookup Online Tools

In addition to the Whois lookup tools mentioned so far, a few online Whois lookup tools are listed as follows:

- SmartWhois available at <http://smartwhois.com>
- Better Whois available at <http://www.betterwhois.com>
- Whois Source available at <http://www.whois.sc>
- Web Wiz available at <http://www.webwiz.co.uk/domain-tools/whois-lookup.htm>
- Network-Tools.com available at <http://network-tools.com>
- Whois available at <http://tools.whois.net>
- DNSstuff available at <http://www.dnsstuff.com>
- Network Solutions Whois available at <http://www.networksolutions.com>
- WebToolHub available at <http://www.webtoolhub.com/tn561381-whois-lookup.aspx>
- Ultra Tools available at <https://www.ultratools.com/whois/home>



Footprinting Methodology

The next phase in footprinting methodology is DNS footprinting.

This section describes how to extract DNS information and the **DNS interrogation** tools.

Extracting DNS Information



Attacker can gather DNS information to determine key hosts in the network and can perform social engineering attacks



DNS records provide important information about location and type of servers

Record Type	Description
A	Points to a host's IP address
MX	Points to domain's mail server
NS	Points to host's name server
CNAME	Canonical naming allows aliases to a host
SOA	Indicate authority for domain
SRV	Service records
PTR	Maps IP address to a hostname
RP	Responsible person
HINFO	Host information record includes CPU type and OS
TXT	Unstructured text records

DNS Interrogation Tools

- <http://www.dnsstuff.com>
- <http://network-tools.com>




Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Extracting DNS Information

DNS footprinting allows you to obtain information about **DNS zone data**. This DNS zone data includes DNS domain names, computer names, IP addresses, and much more about a particular network. The attacker performs **DNS footprinting** on the target network in order to obtain the information about DNS. He or she then uses the gathered DNS information to determine key hosts in the network and then performs social engineering attacks to gather more information.

DNS footprinting can be performed using DNS interrogation tools such as www.DNSstuff.com. By using www.DNSstuff.com, it is possible to extract DNS information about IP addresses, mail server extensions, DNS lookups, Whois lookups, etc. If you want information about a target company, it is possible to extract its range of IP addresses utilizing the **IP routing** lookup of DNS stuff. If the target network allows unknown, unauthorized users to transfer DNS zone data, then it is easy for you to obtain the information about DNS with the help of the DNS interrogation tool.

Once you send the query using the DNS interrogation tool to the **DNS server**, the server will respond to you with a record structure that contains information about the target DNS. DNS records provide important information about location and type of servers.

- A - Points to a host's IP address

- MX - Points to domain's mail server
- NS - Points to host's name server
- CNAME - Canonical naming allows aliases to a host
- SOA - Indicate authority for domain
- SRV - Service records
- PTR - Maps IP address to a hostname
- RP - Responsible person
- HINFO - Host information record includes CPU type and OS

A few more examples of DNS interrogation tools to send a DNS query include:

- <http://www.dnsstuff.com>
- <http://network-tools.com>

Extracting DNS Information

(Cont'd)

This tool is very useful to perform a DNS query on any host. Each domain name (Example: dnsqueries.com) is structured in hosts (ex: dnsqueries.com) and the DNS (Domain Name System) allow to translate the domain name or the hostname in an IP Address to contact via the TCP/IP protocol. There are several types of queries, corresponding to all the implementable types of DNS records such as A record, MX, AAAA, CNAME and SOA.

Perform DNS query

HostName:

Type:

Results for checks on microsoft.com

Host	TTL	Class	Type	Details
microsoft.com	3381	IN	TXT	FbUF6DbkE+Aw1/vi9xgDi8Kv1Izus5v8L6tbIQZkGrQ/rVQKJi8CjQb8TWIE64ey4NJJvj5J65PlggYYNabdQ==
microsoft.com	3381	IN	TXT	v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com include:_spf-ssg-a.microsoft.com ip4:131.107.115.215 ip4:131.107.115.214 ip4:205.248.106.64 ip4:205.248.106.30 ip4:205.248.106.32 ~all
microsoft.com	3381	IN	MX	10 mail.messaging.microsoft.com
microsoft.com	3381	IN	SOA	ns1.msft.net msnhst.microsoft.com 2012071602 300 600 2419200 3600
microsoft.com	3381	IN	A	64.4.11.37
microsoft.com	3381	IN	A	65.55.58.201
microsoft.com	141531	IN	NS	ns5.msft.net
microsoft.com	141531	IN	NS	ns2.msft.net
microsoft.com	141531	IN	NS	ns1.msft.net
microsoft.com	141531	IN	NS	ns3.msft.net
microsoft.com	141531	IN	NS	ns4.msft.net

<http://www.dnsqueries.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Extracting DNS Information (Cont'd)

Source: <http://www.dnsqueries.com>

Perform DNS query available at <http://www.dnsqueries.com> is a tool that allows you to perform a DNS query on any host. Each domain name (example: dnsqueries.com) is structured in hosts (ex: www.dnsqueries.com) and the DNS (Domain Name System) allows anyone to translate the domain name or the hostname in an IP address to contact via the **TCP/IP protocol**. There are several types of queries, corresponding to all the implementable types of DNS records such as a record, MX, AAAA, CNAME, and SOA.

Now let's see how the DNS interrogation tool retrieves information about the DNS. Go to the browser and type <http://www.dnsqueries.com> and press Enter. The DNS query's homesite will be displayed in the browser.

Enter the domain name of your interest in the Perform **DNS query's HostName** field (here we are entering Microsoft.com) and click the Run tool button; the DNS information for Microsoft.com will be displayed as shown in the following figure.

This tool is very useful to perform a DNS query on any host. Each domain name (Example: dnsqueries.com) is structured in hosts (ex: www.dnsqueries.com) and the DNS (Domain Name System) allow everybody to translate the domain name or the hostname in an IP Address to contact via the TCP/IP protocol. There are several types of queries, corresponding to all the implementable types of DNS records such as A record, MX, AAAA, CNAME and SOA.

Perform DNS query

HostName:

Type:

Results for checks on microsoft.com

Host	TTL	Class	Type	Details
microsoft.com	3381	IN	TXT	FbUF6DbkE-Aw1/vi9xgDi8KvriiZes5v8L6tbIQZkGrQ/rVQKJ8CjQbBtWE64ey4NUJvj5J65PlggVYNabdQ--v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com include:_spf-ssg-a.microsoft.com ip4:131.107.115.215 ip4:131.107.115.214 ip4:205.248.106.64 ip4:205.248.106.30 ip4:205.248.106.32 ~all
microsoft.com	3381	IN	MX	10 mail.messaging.microsoft.com
microsoft.com	3381	IN	SOA	ns1.msft.net msnhst.microsoft.com 2012071602 300 600 2419200 3600
microsoft.com	3381	IN	A	64.4.11.37
microsoft.com	3381	IN	A	65.55.58.201
microsoft.com	141531	IN	NS	ns5.msft.net
microsoft.com	141531	IN	NS	ns2.msft.net
microsoft.com	141531	IN	NS	ns1.msft.net
microsoft.com	141531	IN	NS	ns3.msft.net
microsoft.com	141531	IN	NS	ns4.msft.net

FIGURE 2.32: Screenshot showing DNS information for Microsoft.com

DNS Interrogation Tools



 DIG http://www.kloth.net	 DNSWatch http://www.dnswatch.info
 myDNSTools http://www.mynstools.info	 DomainTools http://www.domaintools.com
 Professional Toolset http://www.dnsstuff.com	 DNS http://e-dns.org
 DNS Records http://network-tools.com	 DNS Lookup Tool http://www.webwiz.co.uk
 DNSData View http://www.nirsoft.net	 DNS Query Utility http://www.webmaster-toolkit.com

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



DNS Interrogation Tools

A few more well-known **DNS interrogation** tools are listed as follows:

- DIG available at <http://www.kloth.net>
- myDNSTools available at <http://www.mynstools.info>
- Professional Toolset available at <http://www.dnsstuff.com>
- DNS Records available at <http://network-tools.com>
- DNSData View available at <http://www.nirsoft.net>
- DNSWatch available at <http://www.dnswatch.info>
- DomainTools Pro available at <http://www.domaintools.com>
- DNS available at <http://e-dns.org>
- DNS Lookup Tool available at <http://www.webwiz.co.uk>
- DNS Query Utility available at <http://www.webmaster-toolkit.com>



Footprinting Methodology

The next step after retrieving the DNS information is to gather **network-related** information. So, now we will discuss network footprinting, a method of gathering network-related information.

This section describes how to locate network range, determine the operating system, Traceroute, and the **Traceroute tools**.

Locate the Network Range



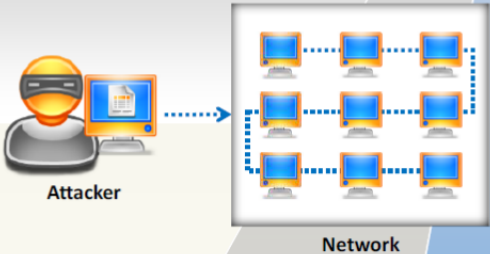
- Network range information obtained assists an attacker to create a **map of the target's network**
- Find the **range of IP addresses** using **ARIN whois database search** tool
- You can find the range of IP addresses and the subnet mask used by the target organization from **Regional Internet Registry (RIR)**

Network Whois Record

Queried whois.arin.net with "n 207.46.232.182"...

```

NetRange:      207.46.0.0 - 207.46.255.255
CIDR:          207.46.0.0/16
OriginAS:
NetName:       MICROSOFT-GLOBAL-NET
NetHandle:     NET-207-46-0-0-1
Parent:        NET-207-0-0-0-0
NetType:       Direct Assignment
NameServer:    NS2.MSFT.NET
NameServer:    NS4.MSFT.NET
NameServer:    NS1.MSFT.NET
NameServer:    NS5.MSFT.NET
NameServer:    NS3.MSFT.NET
RegDate:       1997-03-31
Updated:       2004-12-09
Ref:           http://whois.arin.net/rest/net/NET-207-46-0-0-1
OrgName:       Microsoft Corp
OrgId:         MSFT
Address:       One Microsoft Way
City:          Redmond
StateProv:     WA
PostalCode:    98052
Country:       US
RegDate:       1998-07-10
Updated:       2009-11-10
Ref:           http://whois.arin.net/rest/org/MSFT
OrgAbuseHandle: ABUSE231-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:   +1-425-882-8080
OrgAbuseEmail:   abuse@hotmail.com
OrgAbuseRef:     http://whois.arin.net/rest/poc/ABUSE231-ARIN
                    
```



Attacker Network

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Locate the Network Range

To perform network footprinting, you need to **gather basic** and **important information** about the target organization such as what the organization does, who they work for, and what type of work they perform. The answers to these questions give you an idea about the internal structure of the target network.

After gathering the aforementioned information, an attacker can proceed to find the network range of a target system. He or she can get more detailed information from the appropriate regional registry database regarding IP allocation and the nature of the allocation. An attacker can also determine the subnet mask of the domain. He or she can also trace the route between the system and the target system. Two popular **traceroute tools** are NeoTrace and Visual Route.

Obtaining private IP addresses can be useful for an attacker. The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private Internets: 10.0.0.0–10.255.255.255 (10/8 prefix), 172.16.0.0–172.31.255.255 (172.16/12 prefix), and 192.168.0.0–192.168.255.255 (192.168/16 prefix).

The network range gives you an idea about how the network is, which machines in the networks are alive, and it helps to identify the network topology, access control device, and OS

used in the target network. To find the **network range** of the target network, enter the server IP address (that was gathered in **WHOIS footprinting**) in the ARIN whois database search tool or you can go to the ARIN website (<https://www.arin.net/knowledge/rirs.html>) and enter the server IP in the SEARCH Whois text box. You will get the network range of the target network. If the DNS servers are not set up correctly, the attacker has a good chance of obtaining a list of internal machines on the server. Also, sometimes if an attacker traces a route to a machine, he or she can get the internal IP address of the **gateway**, which might be useful.

Network Whois Record

```
Queried whois.arin.net with "n 207.46.232.182"...

NetRange:      207.46.0.0 - 207.46.255.255
CIDR:          207.46.0.0/16
OriginAS:
NetName:       MICROSOFT-GLOBAL-NET
NetHandle:     NET-207-46-0-0-1
Parent:        NET-207-0-0-0-0
NetType:       Direct Assignment
NameServer:    NS2.MSFT.NET
NameServer:    NS4.MSFT.NET
NameServer:    NS1.MSFT.NET
NameServer:    NS5.MSFT.NET
NameServer:    NS3.MSFT.NET
RegDate:       1997-03-31
Updated:       2004-12-09
Ref:           http://whois.arin.net/rest/net/NET-
207-46-0-0-1
OrgName:       Microsoft Corp
OrgId:         MSFT
Address:       One Microsoft Way
City:          Redmond
StateProv:     WA
PostalCode:    98052
Country:       US
RegDate:       1998-07-10
Updated:       2009-11-10
Ref:           http://whois.arin.net/rest/org/MSFT
OrgAbuseHandle: ABUSE231-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-425-882-8080
OrgAbuseEmail:  abuse@hotmail.com
OrgAbuseRef:    http://whois.arin.net/rest/poc/ABUSE231-ARIN
```

You need to use more than one tool to obtain network information as sometimes a single tool is not capable of delivering the information you want.

Determine the Operating System

Use the **Netcraft** tool to determine the OSes in use by the target organization

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Determine the Operating System

Source: <http://news.netcraft.com>

So far we have collected information about IP addresses, network ranges, server names, etc. of the target network. Now it's time to find out the **OS running** on the **target network**. The technique of obtaining information about the target network OS is called **OS fingerprinting**. The Netcraft tool will help you to find out the OS running on the target network.

Let's see how Netcraft helps you determine the OS of the target network.

Open the <http://news.netcraft.com> site in your browser and type the domain name of your target network in the What's that site running? field (here we are considering the domain name "Microsoft.com"). It displays all the **sites associated** with that domain along with the operating system running on each site.

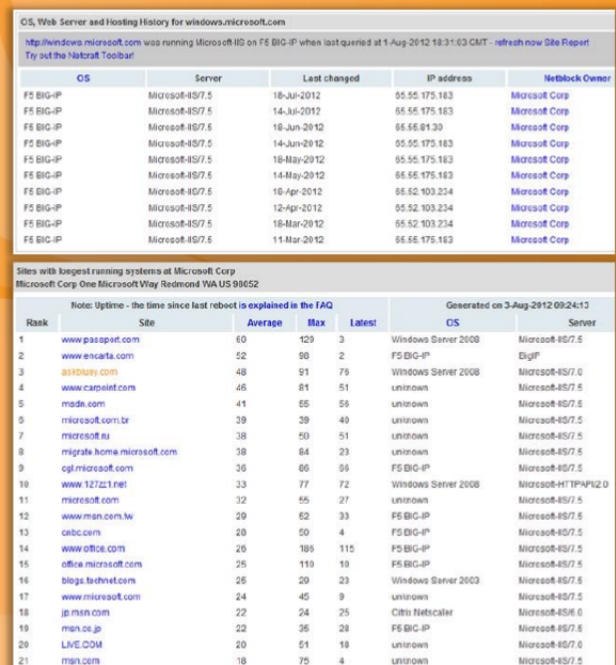


FIGURE 2.33: Netcraft showing the operating system that is in use by Microsoft

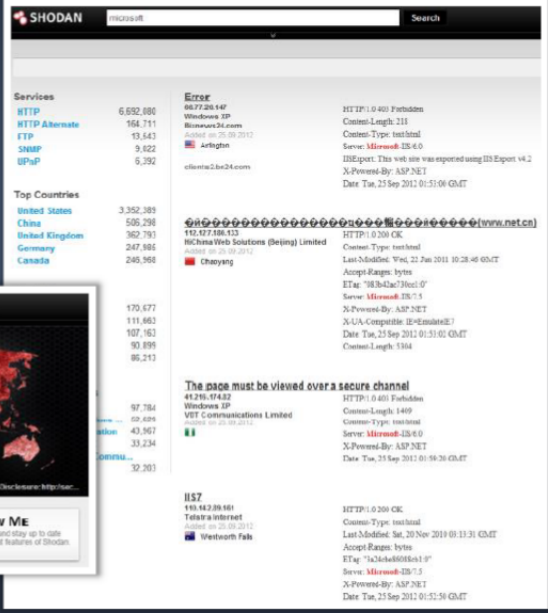
Determine the Operating System



(Cont'd)

Use SHODAN search engine that lets you **find specific computers** (routers, servers, etc.) using a variety of filters







<http://www.shodanhq.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Determine the Operating System (Cont'd)



SHODAN Search Engine

Source: <http://www.shodanhq.com>

Use SHODAN search engine that lets you find specific computers (routers, servers, etc.) using a variety of filters.



FIGURE 2.34: SHODAN Search Engine screenshot

SHODAN

microsoft

Search

Services

HTTP	6,692,080
HTTP Alternate	164,711
FTP	13,543
SNMP	9,022
UPnP	6,392

Top Countries

United States	3,352,389
China	506,298
United Kingdom	362,793
Germany	247,985
Canada	246,968

Top Cities

Englewood	170,677
Beijing	111,663
Columbus	107,163
Dallas	90,899
Seoul	86,213

Top Organizations

Verio Web Hosting	97,784
HiChina Web Solutions ...	52,629
Ecommerce Corporation	43,967
GoDaddy.com, LLC	33,234
Comcast Business Commu...	32,203

Error

66.77.20.147

Windows XP

Biznews24.com

Added on 25.09.2012

Arlington

clients2.bn24.com

HTTP/1.0 403 Forbidden

Content-Length: 218

Content-Type: text/html

Server: Microsoft-IIS/6.0

IISExport: This web site was exported using IIS Export v4.2

X-Powered-By: ASP.NET

Date: Tue, 25 Sep 2012 01:53:00 GMT

112.127.180.133

HiChina Web Solutions (Beijing) Limited

Added on 25.09.2012

Chaoyang

HTTP/1.0 200 OK

Content-Type: text/html

Last-Modified: Wed, 22 Jun 2011 10:28:46 GMT

Accept-Ranges: bytes

ETag: "083b42ac730cc1.0"

Server: Microsoft-IIS/7.5

X-Powered-By: ASP.NET

X-UA-Compatible: IE=EmulateIE7

Date: Tue, 25 Sep 2012 01:53:02 GMT

Content-Length: 5304

The page must be viewed over a secure channel!

41.216.174.82

Windows XP

VDI Communications Limited

Added on 25.09.2012

Wentworth Falls

HTTP/1.0 403 Forbidden

Content-Length: 1409

Content-Type: text/html

Server: Microsoft-IIS/6.0

X-Powered-By: ASP.NET

Date: Tue, 25 Sep 2012 01:59:20 GMT

IIS7

110.142.89.161

Telstra Internet

Added on 25.09.2012

Wentworth Falls

HTTP/1.0 200 OK

Content-Type: text/html

Last-Modified: Sat, 20 Nov 2010 03:13:31 GMT

Accept-Ranges: bytes

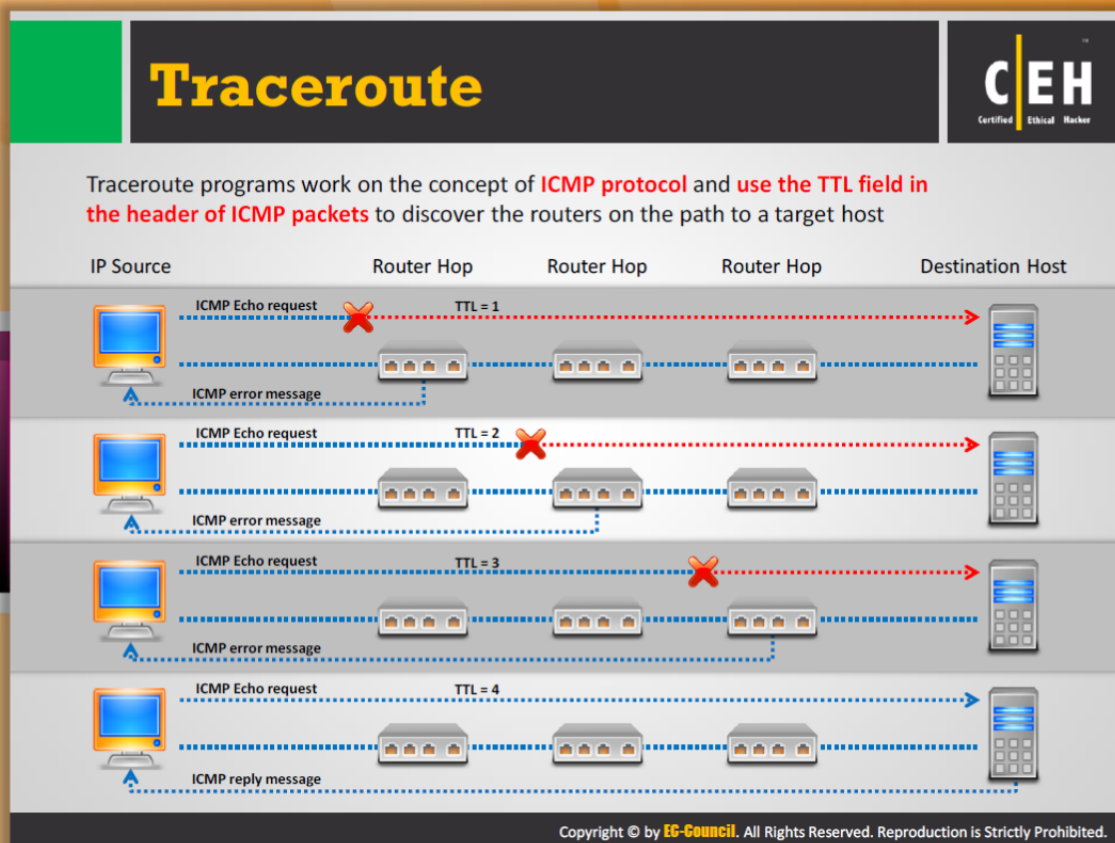
ETag: "3a24cbe86088cb1.0"

Server: Microsoft-IIS/7.5

X-Powered-By: ASP.NET

Date: Tue, 25 Sep 2012 01:52:50 GMT

FIGURE 2.35: SHODAN screenshot



Traceroute

Finding the route of the target host is necessary to test against **man-in-the-middle attacks** and other relative attacks. Therefore, you need to find the route of the target host in the network. This can be accomplished with the help of the Traceroute utility provided with most operating systems. It allows you to trace the path or route through which the target host packets travel in the network.

Traceroute uses the **ICMP protocol** concept and **TTL (Time to Live)** field of IP header to find the path of the target host in the network.

The Traceroute utility can detail the path IP packets travel between two systems. It can trace the number of routers the packets travel through, the round trip time duration in transiting between two routers, and, if the routers have DNS entries, the names of the routers and their network affiliation, as well as the geographic location. It works by exploiting a feature of the Internet Protocol called **Time To Live (TTL)**. The TTL field is interpreted to indicate the maximum number of routers a packet may transit. Each router that handles a packet will decrement the TTL count field in the ICMP header by one. When the count reaches zero, the packet will be discarded and an error message will be transmitted to the originator of the packet.

It sends out a packet destined for the destination specified. It sets the TTL field in the packet to one. The first router in the path receives the packet, decrements the TTL value by one, and if the resulting TTL value is 0, it discards the packet and sends a message back to the originating host to inform it that the packet has been discarded. It records the **IP address** and **DNS name** of that router, and sends out another packet with a TTL value of two. This packet makes it through the first router, then times-out at the next router in the path. This second router also sends an error message back to the originating host. Traceroute continues to do this, and records the IP address and name of each router until a packet finally reaches the target host or until it decides that the host is unreachable. In the process, it records the time it took for each packet to travel round trip to each router. Finally, when it reaches the destination, the normal ICMP ping response will be sent to the sender. Thus, this utility helps to reveal the IP addresses of the intermediate hops in the route of the target host from the source.

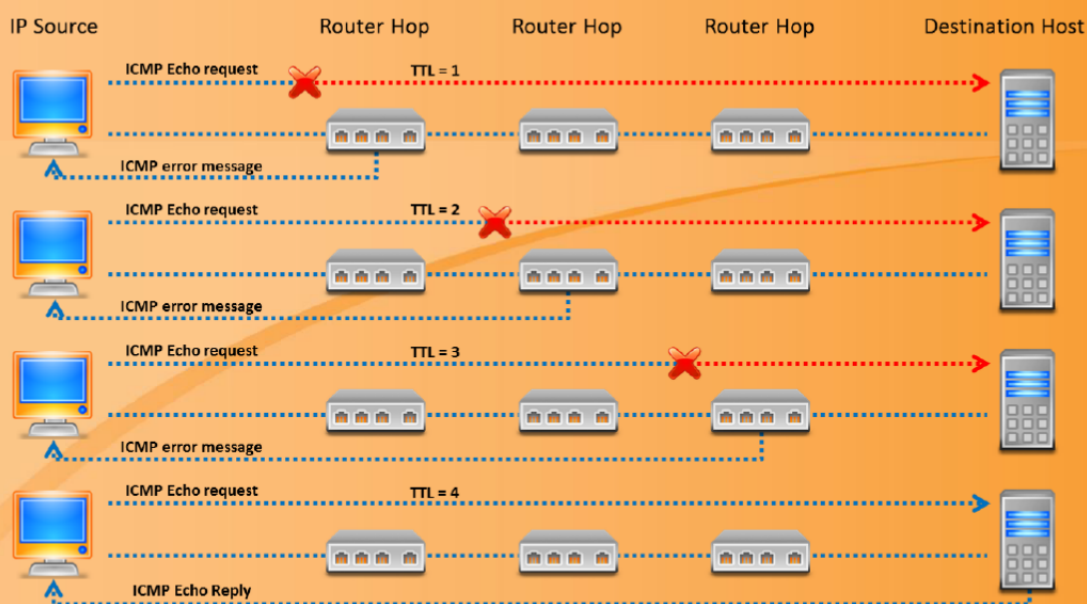


FIGURE 2.36: Working of Traceroute program

How to use the tracert command

Go to the command prompt and type the `tracert` command along with destination IP address or domain name as follows:

```
C:\>tracert 216.239.36.10
```

Tracing route to ns3.google.com [216.239.36.10] over a maximum of 30 hops:

```

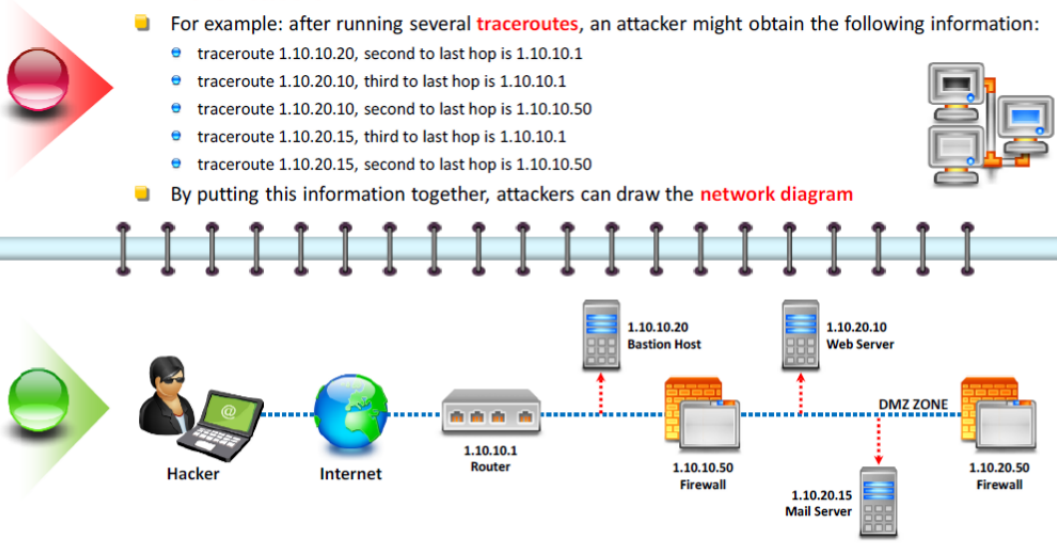
 1  1262 ms   186 ms   124 ms   195.229.252.10
 2  2796 ms  3061 ms  3436 ms  195.229.252.130
 3   155 ms   217 ms   155 ms   195.229.252.114
 4  2171 ms  1405 ms  1530 ms  194.170.2.57
 5  2685 ms  1280 ms   655 ms  dxb-emix-ra.ge6303.emix.ae [195.229.31.99]
 6   202 ms   530 ms   999 ms  dxb-emix-rb.so100.emix.ae [195.229.0.230]
 7  609 ms   1124 ms  1748 ms  iar1-so-3-2-0.Thamesside.cw.net [166.63.214.65]
```

```
8 1622 ms 2377 ms 2061 ms eqixva-google-gige.google.com [206.223.115.21]
9 2498 ms 968 ms 593 ms 216.239.48.193
10 3546 ms 3686 ms 3030 ms 216.239.48.89
11 1806 ms 1529 ms 812 ms 216.33.98.154
12 1108 ms 1683 ms 2062 ms ns3.google.com [216.239.36.10]
Trace complete.
```

Traceroute Analysis



- Attackers conduct traceroute to extract information about: **network topology**, **trusted routers**, and **firewall locations**
- For example: after running several **traceroutes**, an attacker might obtain the following information:
 - traceroute 1.10.10.20, second to last hop is 1.10.10.1
 - traceroute 1.10.20.10, third to last hop is 1.10.10.1
 - traceroute 1.10.20.10, second to last hop is 1.10.10.50
 - traceroute 1.10.20.15, third to last hop is 1.10.10.1
 - traceroute 1.10.20.15, second to last hop is 1.10.10.50
- By putting this information together, attackers can draw the **network diagram**



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Traceroute Analysis

We have seen how the Traceroute utility helps you to find out the **IP addresses** of intermediate devices such as routers, firewalls, etc. present between source and destination. You can draw the network topology diagram by analyzing the **Traceroute results**. After running several traceroutes, you will be able to find out the location of a particular hop in the target network. Let's consider the following traceroute results obtained:

- traceroute 1.10.10.20, second to last hop is 1.10.10.1
- traceroute 1.10.20.10, third to last hop is 1.10.10.1
- traceroute 1.10.20.10, second to last hop is 1.10.10.50
- traceroute 1.10.20.15, third to last hop is 1.10.10.1
- traceroute 1.10.20.15, second to last hop is 1.10.10.50

By analyzing these results, an attacker can draw the network diagram of the target network as follows:

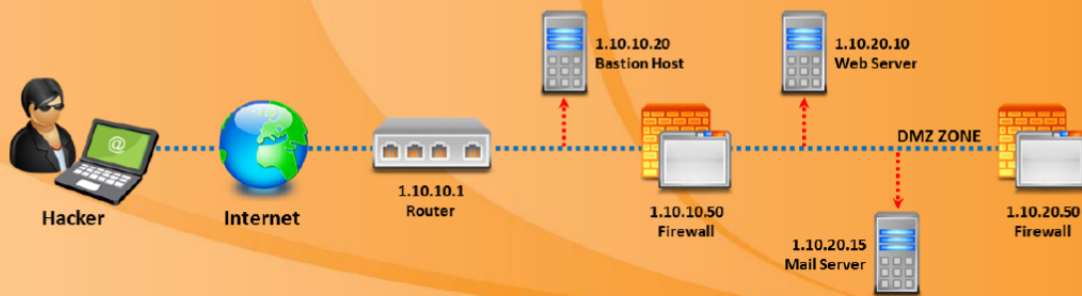


FIGURE 2.37: Diagrammatical representation of the target network

Traceroute Tools

Certified Ethical Hacker

Path Analyzer Pro

http://www.pathanalyzer.com

VisualRoute 2010

http://www.visualroute.com

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Traceroute Tools

Path Analyzer Pro and **VisualRoute 2010** are the two tools similar to Traceroute intended to traceroute the target host in a network.



Path Analyzer Pro

Source: <http://www.pathanalyzer.com>

Path Analyzer Pro is a **graphical-user-interface-based** trace routing tool that shows you the route from source to destination graphically. It also provides information such as the hop number, its IP address, hostname, ASN, network name, % loss, latency, avg. latency, and std. dev. about each hop in the path. You can also map the location of the IP address in the network with this tool. It allows you to detect filters, stateful firewalls, and other anomalies automatically in the network.

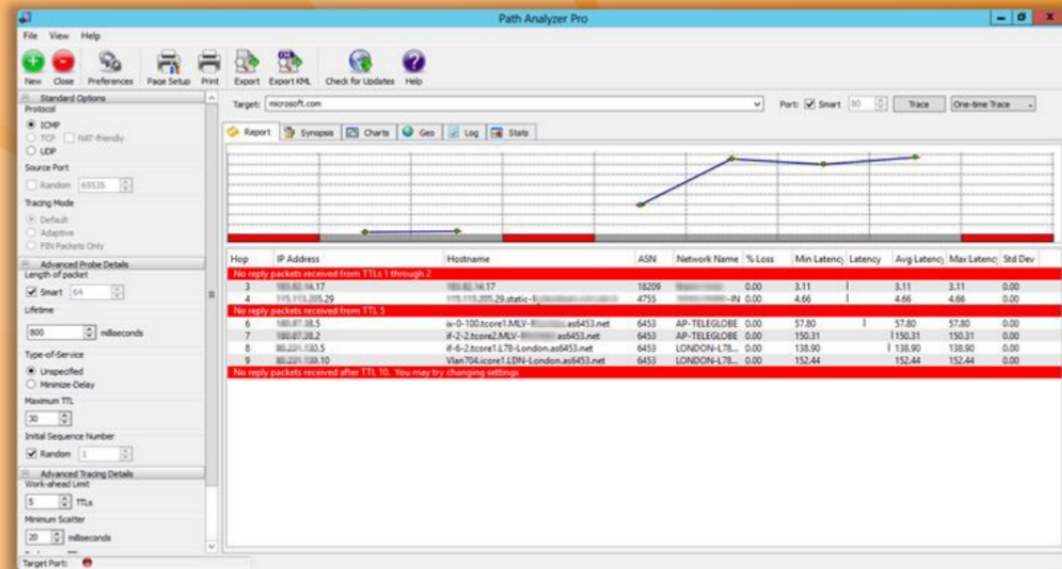


FIGURE 2.38: Path Analyzer Pro screenshot



VisualRoute 2010

Source: <http://www.visualroute.com>

This is another graphical-user-based tracing tool that displays **hop-by-hop analysis**. It enables you to identify the geographical location of the routers, servers, and other IP devices. It is able to provide the **tracing information** in three forms: as an overall analysis, in a data table, and as a geographical view of the routing. The data table contains information such as hop number, IP address, node name, geographical location, etc. about each hop in the route.

Features:

- Hop-by-hop traceroutes
- Reverse tracing
- Historical analysis
- Packet loss reporting
- Reverse DNS
- Ping plotting
- Port probing
- Firefox and IE plugin

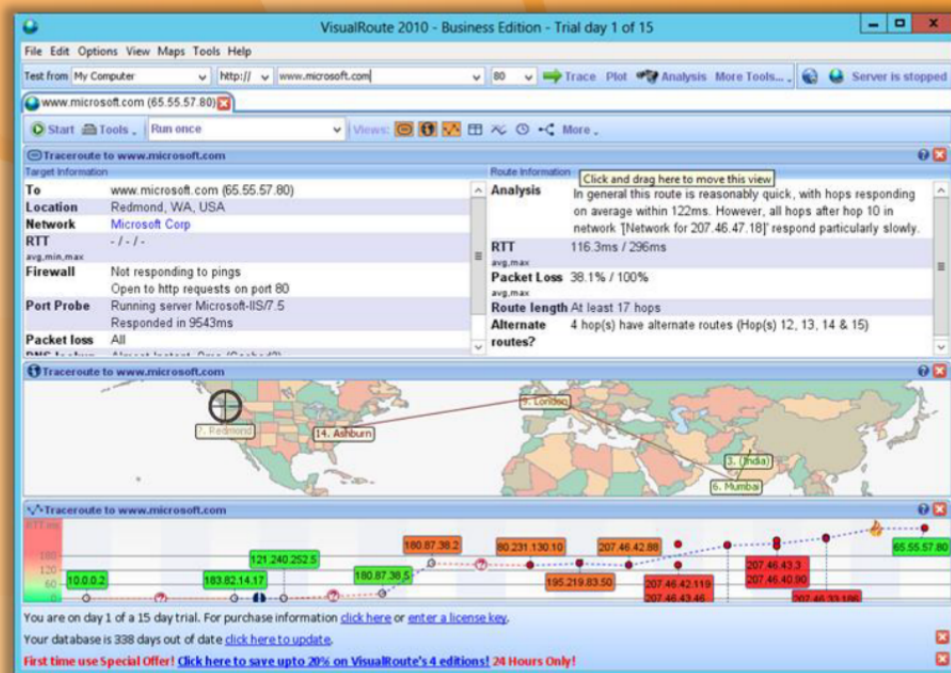


FIGURE 2.39: VisualRoute 2010 screenshot

Traceroute Tools

(Cont'd)



 Network Pinger http://www.networkpinger.com	 Magic NetTrace http://www.tialsoft.com
 GEOSpider http://www.oreware.com	 3D Traceroute http://www.d3tr.de
 vTrace http://vtrace.pl	 AnalogX HyperTrace http://www.analogx.com
 Trout http://www.mcafee.com	 Network Systems Traceroute http://www.net.princeton.edu
 Roadkil's Trace Route http://www.roadkil.net	 Ping Plotter http://www.pingplotter.com

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Traceroute Tools (Cont'd)

A few more traceroute tools similar to Path **Analyzer Pro** and VisualRoute 2010 are listed as follows:

- Network Pinger available at <http://www.networkpinger.com>
- GEOSpider available at <http://www.oreware.com>
- vTrace available at <http://vtrace.pl>
- Trout available at <http://www.mcafee.com>
- Roadkil's Trace Route available at <http://www.roadkil.net>
- Magic NetTrace available at <http://www.tialsoft.com>
- 3D Traceroute available at <http://www.d3tr.de>
- AnalogX HyperTrace available at <http://www.analogx.com>
- Network Systems Traceroute available at <http://www.net.princeton.edu>
- Ping Plotter available at <http://www.pingplotter.com>



Footprinting Methodology

So far we have discussed various techniques of gathering information either with the help of online resources or tools. Now we will discuss footprinting through **social engineering**, the art of grabbing information from people by manipulating them.

This section covers the social engineering concept and techniques used to gather information.

Footprinting through Social Engineering



- Social engineering is the art of **convincing people to reveal confidential information**
- Social engineers depend on the fact that **people are unaware** of their valuable information and are careless about protecting it



Social engineers attempt to gather:

- Credit card details and social security number
- User names and passwords
- Other personal information
- Security products in use
- Operating systems and software versions
- Network layout information
- IP addresses and names of servers



Social engineers use these techniques:

- Eavesdropping
- Shoulder surfing
- Dumpster diving
- Impersonation on social networking sites



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Footprinting through Social Engineering

Social engineering is a **totally non-technical process** in which an attacker tricks a person and obtains confidential information about the target in such a way that the target is unaware of the fact that someone is stealing his or her **confidential information**. The attacker actually plays a cunning game with the target to obtain confidential information. The attacker takes advantage of the helping nature of people and their weakness to provide confidential information.

To perform social engineering, you first need to **gain the confidence of an authorized user** and then trick him or her into revealing confidential information. The basic goal of social engineering is to obtain required confidential information and then use that information for hacking attempts such as gaining unauthorized access to the system, identity theft, industrial espionage, network intrusion, commit frauds, etc. The information obtained through social engineering may include credit card details, social security numbers, usernames and passwords, other personal information, operating systems and software versions, IP addresses, names of servers, network layout information, and much more. Social engineers use this information to hack a system or to commit fraud.

Social engineering can be performed in many ways such as **eavesdropping**, shoulder surfing, dumpster diving, impersonation on social networking sites, and so on.

Collect Information Using **Eavesdropping**, **Shoulder Surfing**, and **Dumpster Diving**





Eavesdropping

- Eavesdropping is **unauthorized listening of conversations** or reading of messages
- It is interception of any form of communication such as audio, video, or written

1



Shoulder Surfing

- Shoulder surfing is the procedure where the **attackers look over the user's shoulder** to gain critical information
- Attackers gather information such as passwords, personal identification number, account numbers, credit card information, etc.

2



Dumpster Diving

- Dumpster diving is **looking for treasure in someone else's trash**
- It involves collection of phone bills, contact information, financial information, operations related information, etc. from the target company's trash bins, printer trash bins, user desk for sticky notes, etc.

3

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Collect Information using Eavesdropping, Shoulder Surfing, and Dumpster Diving

As mentioned previously eavesdropping, shoulder surfing, and dumpster driving are the three techniques used to collect information from people using social engineering. Let's discuss these social engineering techniques to understand how they can be performed to obtain confidential information.



Eavesdropping

Eavesdropping is the act of **secretly listening** to the conversations of people over a phone or videoconference without their consent. It also includes reading secret messages from communication media such as instant messaging or fax transmissions. Thus, it is basically the act of intercepting communication without the consent of the communicating parties. The attacker gains confidential information by tapping the phone conversation, and intercepting audio, video, or written communication.



Shoulder Surfing

With this technique, an **attacker stands** behind the victim and secretly observes the victim's activities on the computer such as keystrokes while entering usernames, passwords, etc.

This technique is commonly used to gain passwords, PINs, security codes, account numbers, credit card information, and similar data. It can be performed in a crowded place as it is relatively easy to stand behind the victim without his or her knowledge.



Dumpster Diving

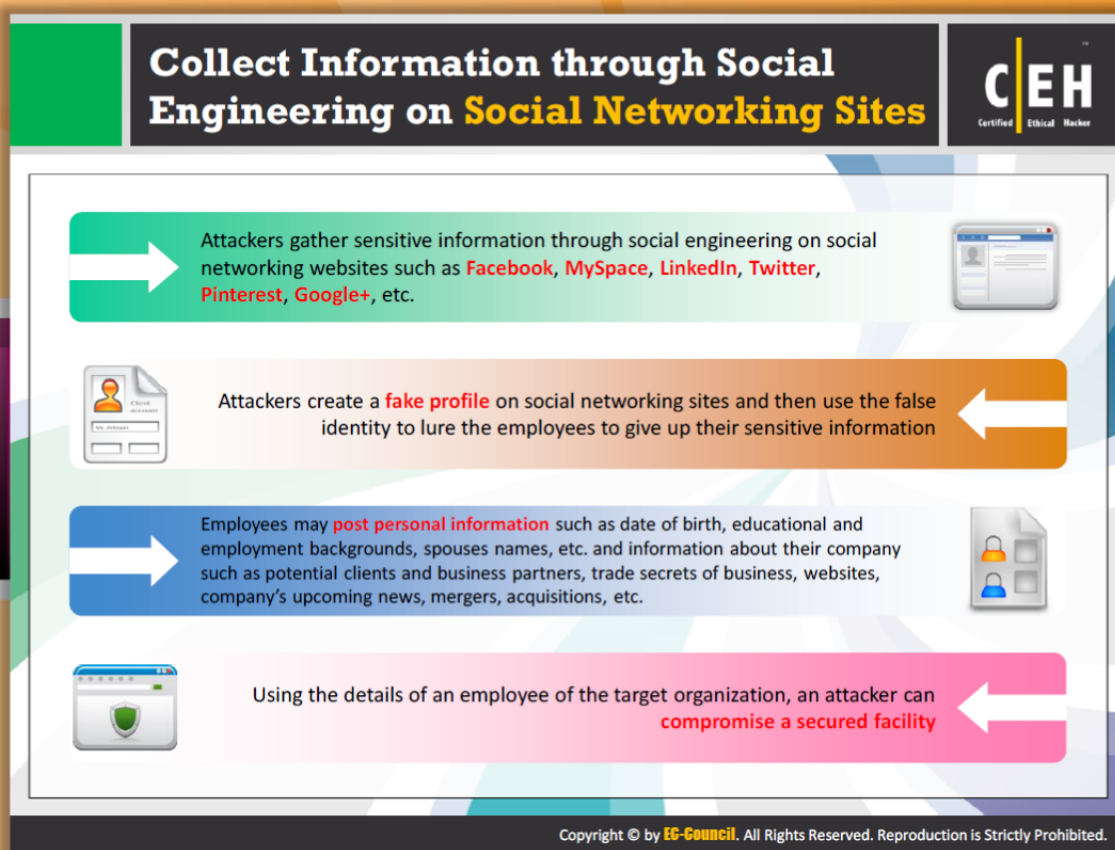
This technique is also known as **trashing**, where the attacker looks for information in the target company's dumpster. The attacker may **gain vital information** such as phone bills, contact information, financial information, operations-related information, printouts of source codes, printouts of sensitive information, etc. from the target company's trash bins, printer trash bins, and sticky notes at users' desks, etc. The obtained information can be helpful for the attacker to commit attacks.



Footprinting Methodology

Though footprinting through social networking sites sounds similar to **footprinting** through social engineering, there are some differences between the two methods. In footprinting through social engineering, the attacker tricks people into revealing information whereas in footprinting through social networking sites, the attacker gathers information available on social networking sites. Attackers can even use **social networking** sites as a medium to perform social engineering attacks.

This section explains how and what information can be collected from social networking sites by means of social engineering.

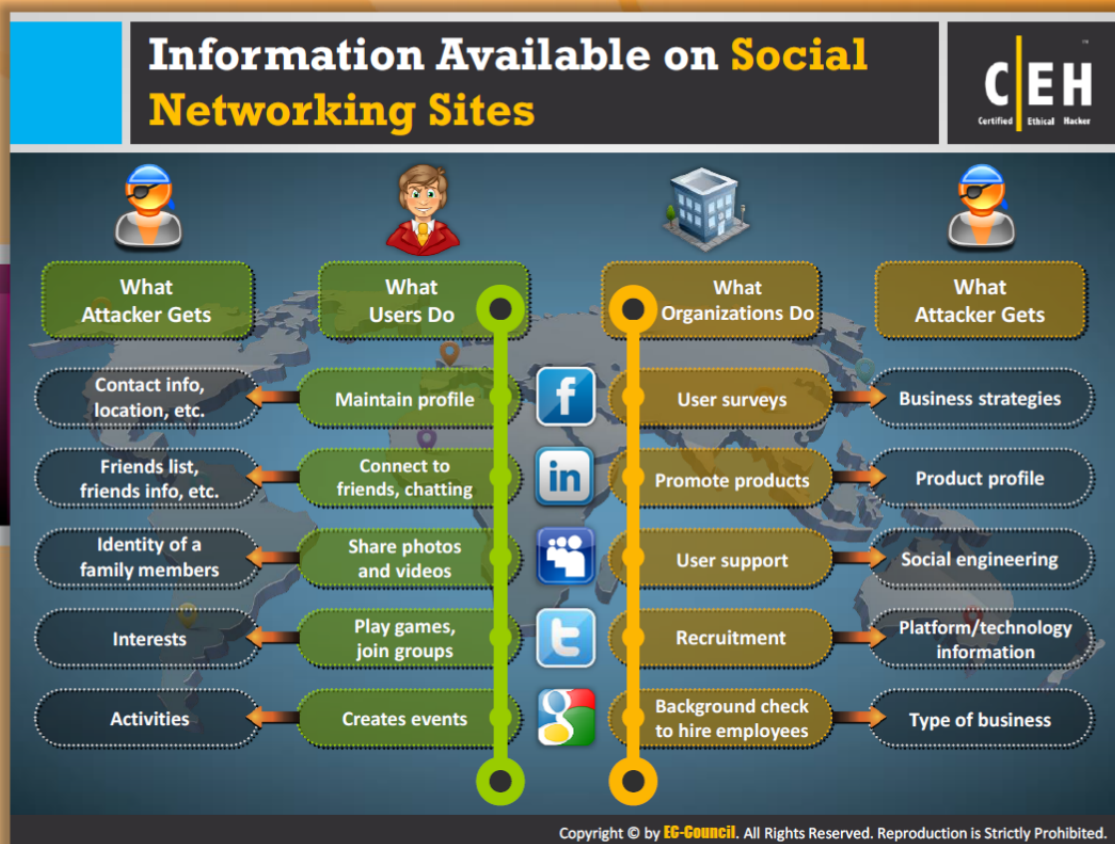


Collect Information through Social Engineering on Social Networking Sites

Social networking sites are the **online services**, platforms, or sites that allow people to connect with each other and to build social relations among people. The use of social networking sites is increasing rapidly. Examples of social networking sites include Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+, and so on. Each social networking site has its own purpose and features. One site may be intended to connect friends, family, etc. and another may be intended to share professional profiles, etc. These social networking sites are open to everyone. Attackers may take advantage of these to **grab sensitive information** from users either by browsing through users' public profiles or by creating a fake profile and tricking user to believe him or her as a genuine user. These **sites allow people** to stay connected with others, to maintain professional profiles, and to share the information with others. On social networking sites, people may post information such as date of birth, educational information, employment backgrounds, spouse's names, etc. and companies may post information such as potential partners, websites, and upcoming news about the company.

For an attacker, these **social networking sites** can be great sources to find information about the target person or the company. These sites help an attacker to collect only the information uploaded by the person or the company. Attackers can easily access public pages of these

accounts on the sites. To obtain more information about the target, attackers may create a fake account and use social engineering to lure the victim to reveal more information. For example, the attacker can send a friend request to the target person from the **fake account**; if the victim accepts the request, then the attacker can access even the restricted pages of the target person on that website. Thus, social networking sites prove to be a valuable information resource for attackers.



Information Available on Social Networking Sites

So far, we have discussed how an attacker can grab information from social networking sites; now we will discuss what information an attacker can get from social networking sites.

People usually maintain profiles on **social networking** sites in order to provide basic information about them and to get connected with others. The profile generally contains information such as name, contact information (mobile number, email ID), friends' information, information about family members, their interests, activities, etc. People usually connect to friends and chat with them. Attackers can gather sensitive information through their chats. Social networking sites also allow people to share photos and videos with their friends. If the people don't set their privacy settings for their **albums**, then **attackers** can see the pictures and videos shared by the victim. Users may join groups to play games or to share their views and interests. Attackers can **grab information** about a victim's interests by tracking their groups and then can trap the victim to reveal more information. Users may create events to notify other users of group about upcoming occasions. With these events, attackers can reveal the victim's activities. Like individuals, organizations also use social networking sites to connect with people, promote their products, and to gather feedback about their products or services, etc. The

activities of an organization on the social networking sites and the respective information that an **attacker** can grab are as follows:

What Organizations Do	What Attacker Gets
User surveys	Business strategies
Promote products	Product profile
User support	Social engineering
Background check to hire employees	Type of business

TABLE 2.1: What organizations Do and What Attacker Gets



Collecting Facebook Information

Facebook is one of the **world's largest social networking sites**, having more than **845 million** monthly active users all over the world. It allows people to create their personal profile, add friends, exchange instant messages, create or join various groups or communities, and much more. An attacker can grab all the information provided by the victim on Facebook. To grab information from Facebook, the attacker should have an active account. The attacker should login to his/her account, and search for either the target person or **organization profile**. Browsing the target person's profile may reveal a lot of useful information such as phone number, email ID, friend information, educational details, professional details, his interests, photos, and much more. The attacker can use this information for further hacking planning, such as **social engineering**, to reveal more information about the target.

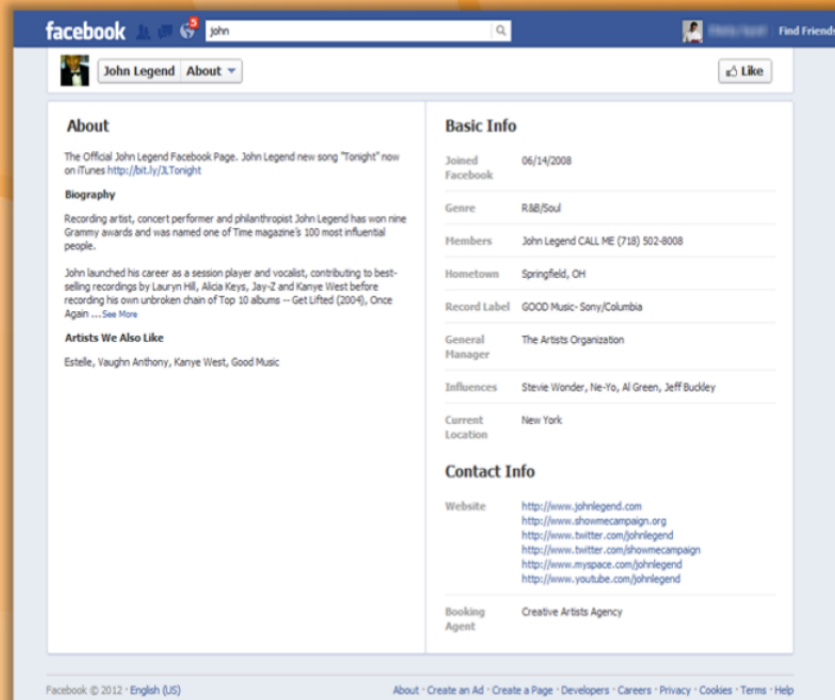


FIGURE 2.40: Facebook screenshot



Collecting Twitter Information

Twitter is another popular **social networking site** used by people to send and read **text-based messages**. It allows you to follow your friends, experts, favorite celebrities, etc. This site also can be a great source for an attacker to get information about the target person. This is helpful in extracting information such as personal information, friend information, activities of the target posted as tweets, whom the target is following, the followers of the user, **photos uploaded**, etc. The attacker may get meaningful information from the target user's tweets.

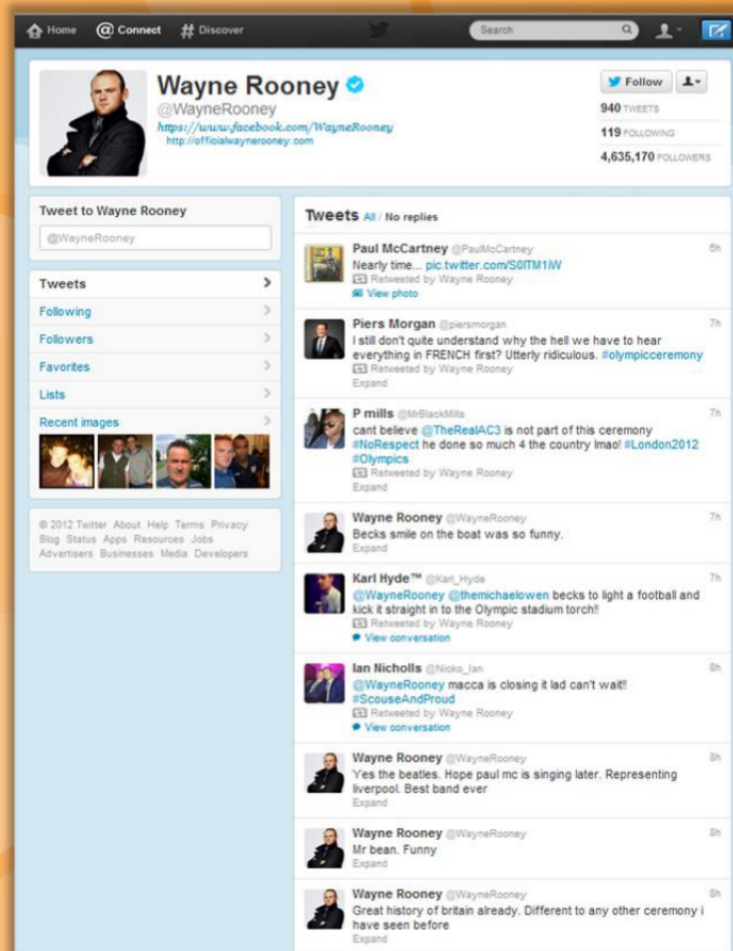


FIGURE 2.41: Twitter showing user's tweets

Collecting LinkedIn Information

**CEH**
Certified Ethical Hacker

161 million members in over 200 countries



**2** new members join every second

**2,447** employees located around the world

**\$522** million revenue for 2011

**2** million companies have LinkedIn company pages

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Collecting LinkedIn Information

Similar to Facebook and Twitter, LinkedIn is another social networking site for professionals. It allows people to create and manage their **professional profile** and identity. It allows its users to build and engage with their professional network. Hence, this can be a great information resource for the attacker. The attacker may get information such as **current employment** details, past employment details, education details, contact details, and much more about the target person. The attacker can collect all this information with the **footprinting** process.

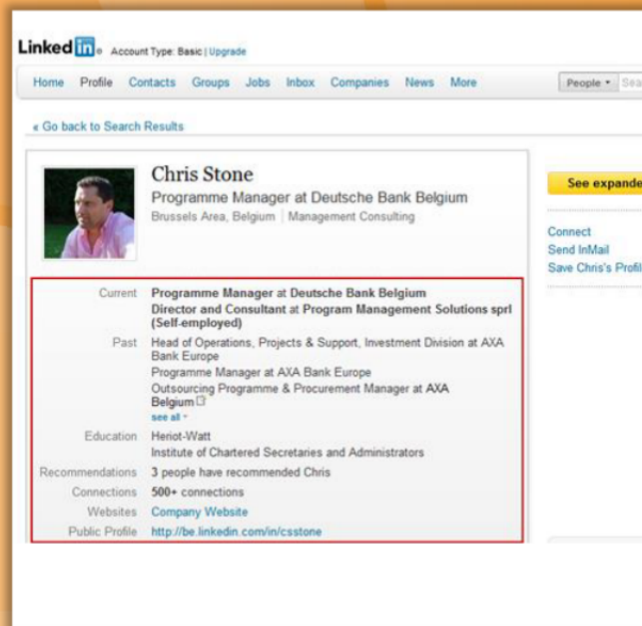


FIGURE 2.42: LinkedIn showing user's professional profile and identity



Collecting YouTube Information

YouTube is a **website** that allows you to upload, view, and share videos all over the world. The attacker can search for the videos related to the target and may collect information from them.

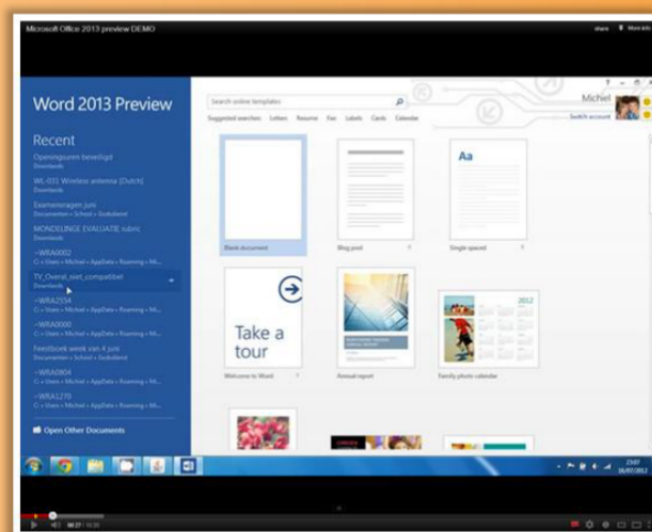


FIGURE 2.43: Youtube showing videos related to target

Tracking Users on Social Networking Sites



- Users may use **fake identities** on social networking sites. Attackers use tools such as **Get Someones IP** or **IP-GRABBER** to track users' real identity
- Steps to get someone's IP address through chat on Facebook using **Get Someones IP** tool:
 - Go to <http://www.myiptest.com/staticpages/index.php/how-about-you>
 - Three fields exist:



Link for Person

Copy the **generated link** of this field and send it to the target via **chat** to get IP address



Redirect URL

Enter any **URL** you want the target to redirect to



Link for you

Open the URL in this field and keep checking for **target's IP**



Link for person: <http://www.myiptest.com/index.php?id=zdeujbg1f2&dr=www.gmail.com&dr=yahoo.com&RedirectURL=http://www.gmail.com>

Redirect URL: <http://www.gmail.com>

Link for you: http://www.myiptest.com/staticpages/index.php/how-about-you?id=zdeujbg1f2&ahow_ip

Link ID	IP	Proxy	Refer	Date/Time
zdeujbg1f2	85.93.218.204	NO	NO	2012-08-06 13:04:44

<http://www.myiptest.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Tracking Users on Social Networking Sites

In order to protect themselves from **Internet fraud** and **attacks**, people with little knowledge about Internet crimes may use fake identities on social networking sites. In such cases, you will not get exact information about the target user. So to determine the real identity of the target user, you can use tools such as Get Someone's **IP** or **IP-GRABBER** to track users' real identities.

If you want to trace the identity of particular user, then do the following:

- Open your web browser, paste the URL, and press Enter:
<http://www.myiptest.com/staticpages/index.php/how-about-you>
- Notice the three fields at the bottom of the web page, namely **Link for person**, **Redirect URL**: **http://**, and **Link for you**.
 - To get real **IP address** of the target, copy the generated link of the **Link for person** field and send it to the target via chat.
 - Enter any **URL** you want the target to redirect to in the **Redirect link**: **http://** field.
 - Open the **URL** present in the **Link for you** field in another window, to monitor the target's IP address details and additional details.

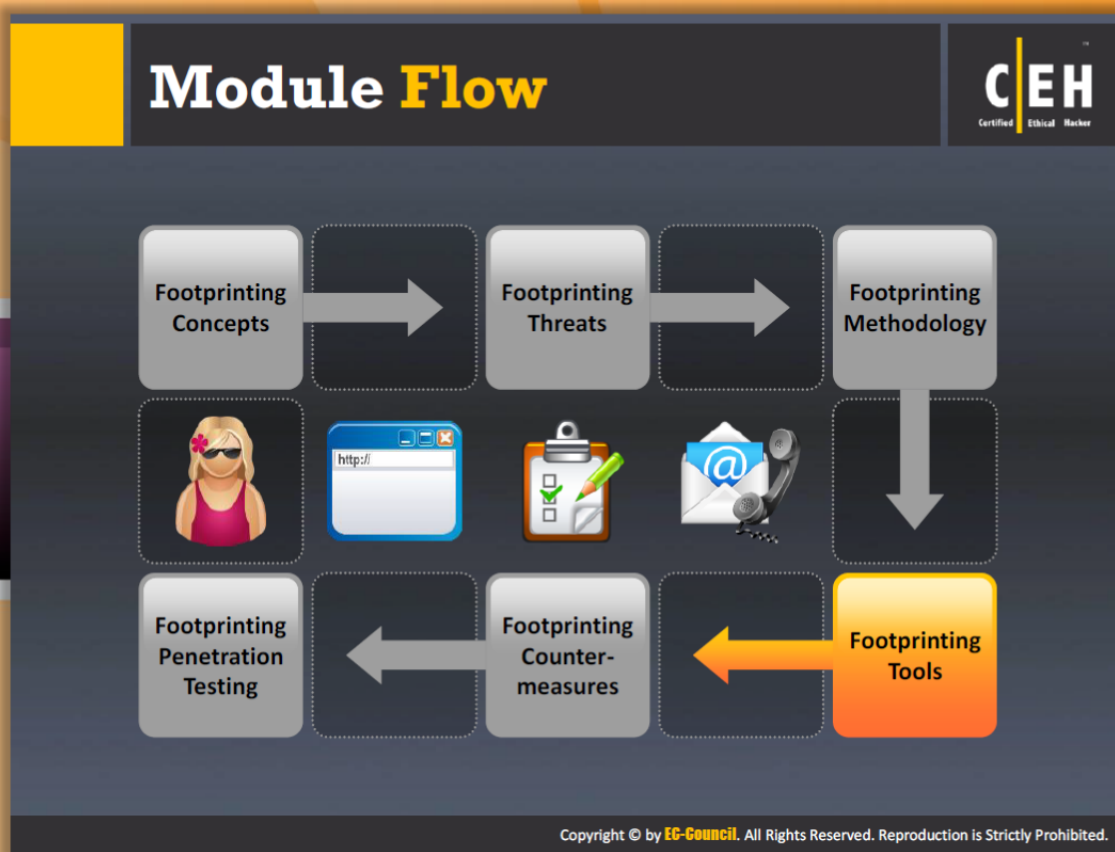
Link for person:

Redirect URL:

Link for you:

Link ID	IP	Proxy	Refer	Date/Time
zdeujbg1f2	85.93.218.204	NO	NO	2012-08-06 13:04:44

FIGURE 2.44: Tracing identity of user's



Module Flow

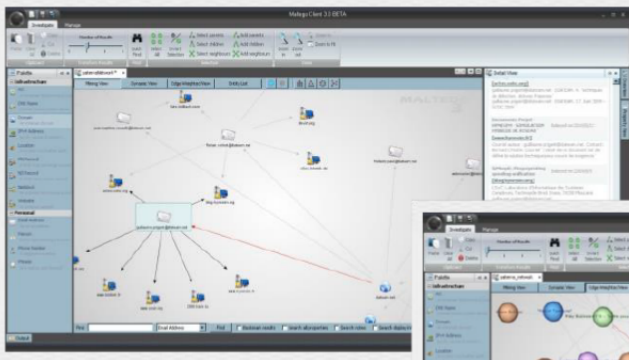
Footprinting can be performed with the help of tools. Many organizations offer tools that make information gathering an easy job. These tools ensure the maximum

 Footprinting Concepts	 Footprinting Tools
 Footprinting Threats	 Footprinting Countermeasures
 Footprinting Methodology	 Footprinting Penetration Testing

This section describes tools intended for grabbing information from various sources.

Footprinting Tool: Maltego



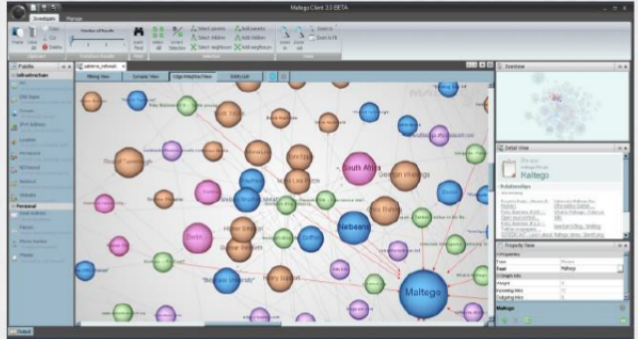


Internet Domain

<http://www.paterva.com>



Maltego is a program that can be used to determine the **relationships and real world links** between people, groups of people (social networks), companies, organizations, websites, Internet infrastructure, phrases, documents, and files



Personal Information

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



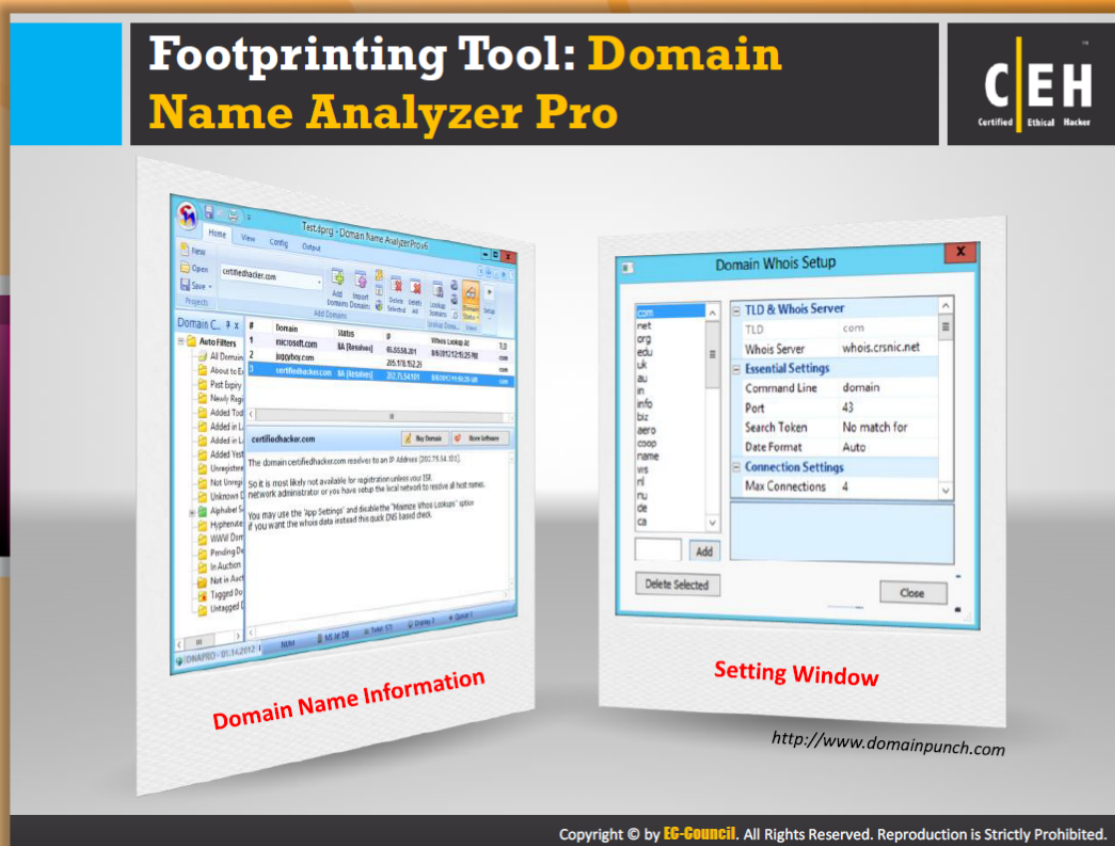
Footprinting Tool: Maltego

Source: <http://paterva.com>

Maltego is an open source **intelligence** and **forensics application**. It can be used for the information gathering phase of all **security-related work**. Maltego is a platform developed to deliver a clear threat picture to the environment that an organization owns and operates. It can be used to determine the relationships and real-world links between people, social networks, companies, organizations, websites, Internet infrastructure (domains, DNS names, Netblocks, IP addresses), phrases, affiliations, documents, and files.



FIGURE 2.45: Maltego showing Internet Domain and personal information

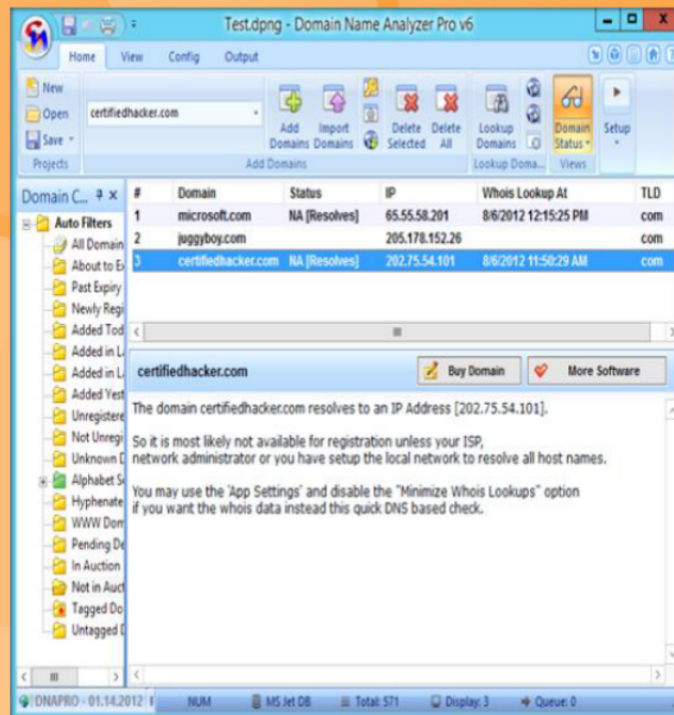


Footprinting Tool: Domain Name Analyzer Pro

Source: <http://www.domainpunch.com>

Domain Name Analyzer Professional is **Windows software** for finding, managing, and maintaining multiple domain names. It supports the display of additional data (expiry and creation dates, name server information), tagging domains, secondary whois lookups (for thin model whois TLDs like COM, NET, TV).

The following is a screenshot of the Domain Name **Analyzer Pro** tool showing domain name information:



Domain Name Information

FIGURE 2.46: Domain Name Analyzer Pro software showing Domain Name Information

Footprinting Tool: Web Data Extractor



- Extract targeted **company contact data** (email, phone, fax) from web for responsible b2b communication
- Extract **URL, meta tag** (title, description, keyword) for website promotion, search directory creation, web research

Phone Numbers

Meta Tags

Fax

<http://www.webextractor.com>

Copyright © by **EG-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Footprinting Tool: Web Data Extractor

Source: <http://www.webextractor.com>

Web Data Extractor is a **data extractor tool**. It extracts targeted company contact data (email, phone, and fax) from the web, extracts the **URL** and **meta tag** (title, desc, keyword) for website promotion, searches directory creation, etc. The following is a screenshot of the **Web Data Extractor** showing meta tags:

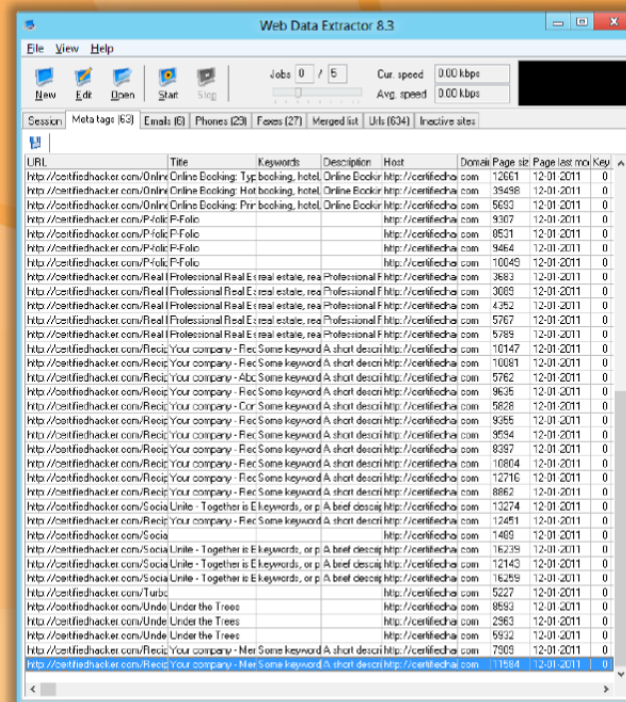


FIGURE 2.47: Web Data Extractor showing meta tags

Additional Footprinting Tools



 Prefix Whols http://pwhois.org	 Netmask http://www.phenoelit-us.org
 NetScanTools Pro http://www.netscantools.com	 Binging http://www.blueinfy.com
 Tctrace http://www.phenoelit-us.org	 Spiderzilla http://spiderzilla.mozdev.org
 Autonomous System Scanner (ASS) http://www.phenoelit-us.org	 Sam Spade http://www.majorgeeks.com
 DNS DIGGER http://www.dnsdigger.com	 Robtex http://www.robtex.com

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Additional Footprinting Tools

In addition to the footprinting tools mentioned previously, a few more tools are listed as follows:

- Prefix Whols available at <http://pwhois.org>
- NetScanTools Pro available at <http://www.netscantools.com>
- Tctrace available at <http://www.phenoelit-us.org>
- Autonomous System Scanner (ASS) available at <http://www.phenoelit-us.org>
- DNS DIGGER available at <http://www.dnsdigger.com>
- Netmask available at <http://www.phenoelit-us.org>
- Binging available at <http://www.blueinfy.com>
- Spiderzilla available at <http://spiderzilla.mozdev.org>
- Sam Spade available at <http://www.majorgeeks.com>
- Robtex available at <http://www.robtex.com>

Additional Footprinting Tools (Cont'd)



 Dig Web Interface http://www.digwebinterface.com	 SpiderFoot http://www.binarypool.com
 Domain Research Tool http://www.domainresearchtool.com	 CallerIP http://www.calleripro.com
 ActiveWhois http://www.johnru.com	 Zaba Search http://www.zabasearch.com
 yoName http://yonline.com	 GeoTrace http://www.nabber.org
 Ping-Probe http://www.ping-probe.com	 DomainHostingView http://www.nirsoft.net

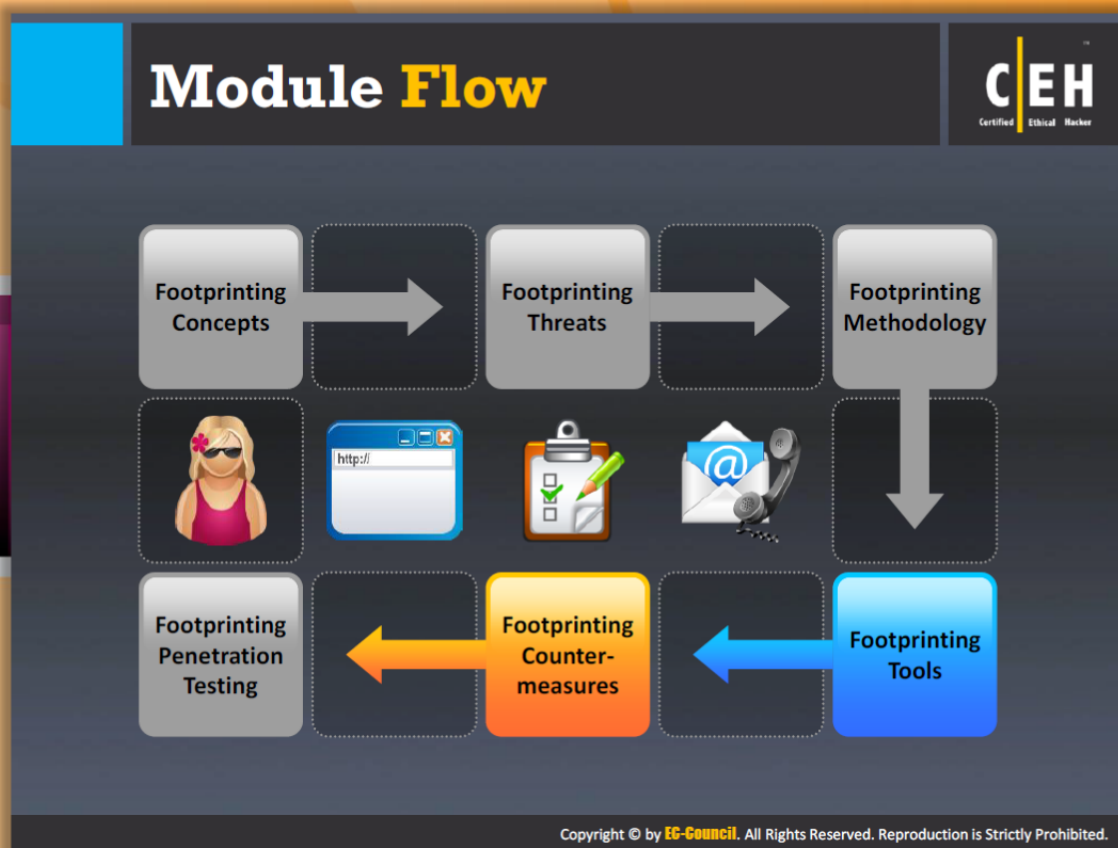
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Additional Footprinting Tools (Cont'd)

Additional **footprinting** tools that are helpful in gathering information about the target person or organization are listed as follows:

- Dig Web Interface available at <http://www.digwebinterface.com>
- Domain Research Tool available at <http://www.domainresearchtool.com>
- ActiveWhois available at <http://www.johnru.com>
- yoName available at <http://yonline.com>
- Ping-Probe available at <http://www.ping-probe.com>
- SpiderFoot available at <http://www.binarypool.com>
- CallerIP available at <http://www.calleripro.com>
- Zaba Search available at <http://www.zabasearch.com>
- GeoTrace available at <http://www.nabber.org>
- DomainHostingView available at <http://www.nirsoft.net>

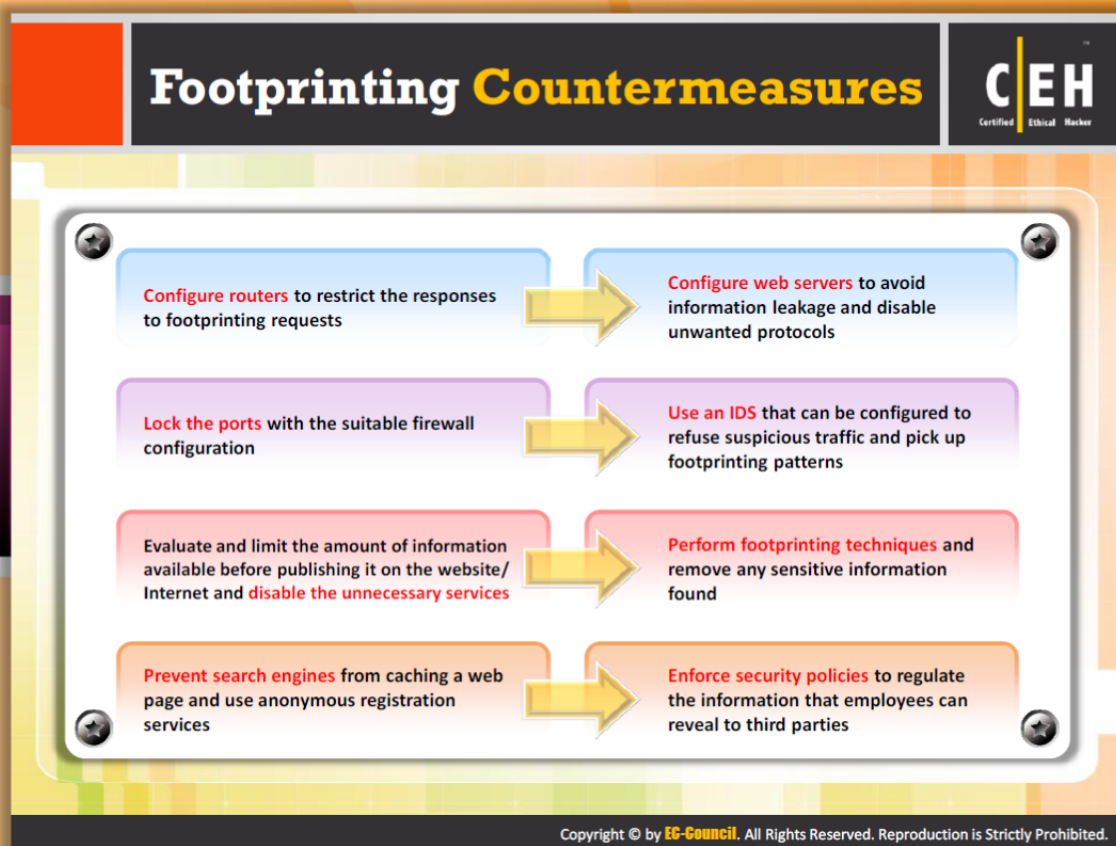


Module Flow

So far we have discussed the importance of footprinting, various ways in which footprinting can be performed, and the tools that can be used for footprinting. Now we will discuss the **countermeasures** to be applied in order to avoid sensitive information disclosure.

 Footprinting Concepts	 Footprinting Tools
 Footprinting Threats	 Footprinting Countermeasures
 Footprinting Methodology	 Footprinting Penetration Testing

This section lists various footprinting countermeasures to be applied at various levels.



Footprinting Countermeasures

Footprinting countermeasures are the measures or actions taken to counter or offset information disclosure. A few footprinting countermeasures are listed as follows:

- Configure routers to restrict the responses to footprinting requests.
- Lock the ports with suitable firewall configuration.
- Evaluate and limit the amount of information available before publishing it on the **website/Internet** and disable the unnecessary services.
- Prevent search engines from caching a webpage and use anonymous registration services.
- Configure web servers to avoid information leakage and disable unwanted protocols.
- Use an IDS that can be configured to refuse **suspicious traffic** and pick up footprinting patterns.
- Perform footprinting techniques and remove any sensitive information found.
- Enforce security policies to regulate the information that employees can reveal to third parties.

Footprinting Countermeasures (Cont'd)



- ✓ Set apart **internal DNS** and **external DNS**
- ✓ Disable **directory listings** and use split-DNS
- ✓ Educate **employees** about various social engineering tricks and risks
- ✓ Restrict **unexpected input** such as `| ; < >`
- ✓ Avoid **domain-level** cross-linking for the critical assets
- ✓ **Encrypt** and **password protect** the sensitive information

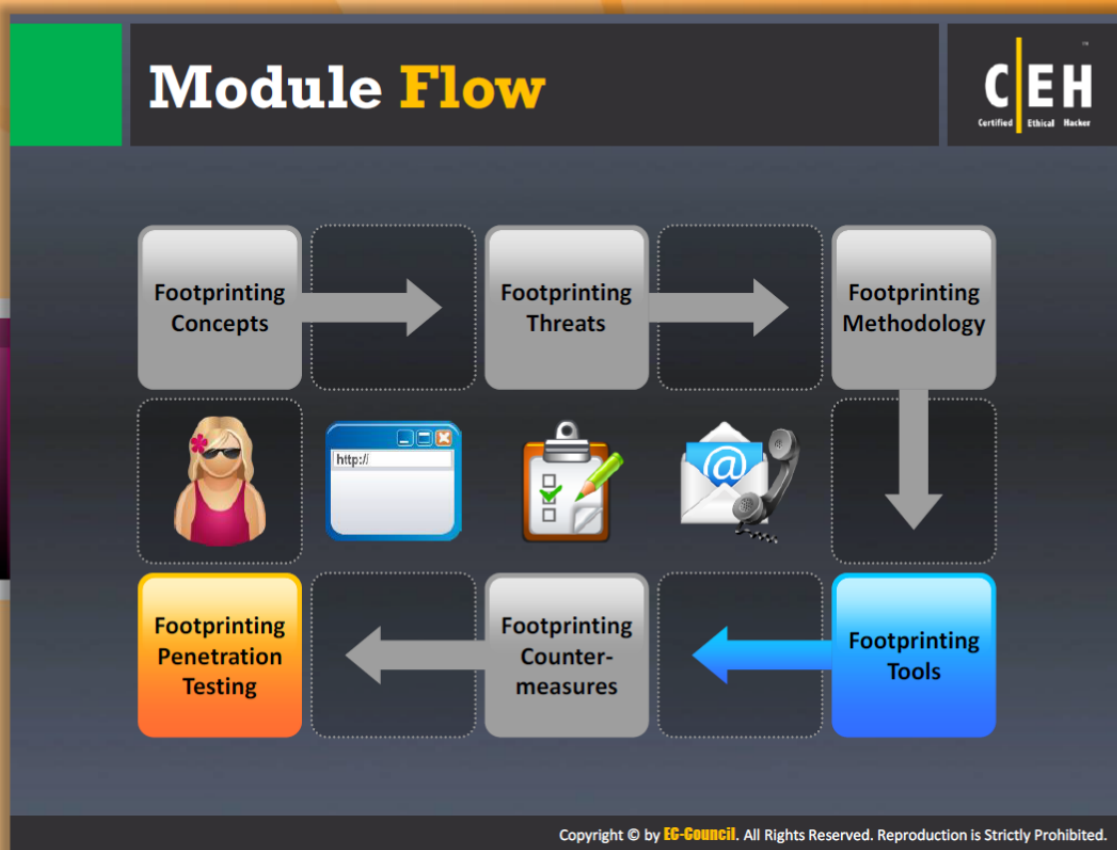
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Footprinting Countermeasures (Cont'd)

In addition to the countermeasures mentioned previously, you can apply the following countermeasures as well:

- Set apart the internal DNS and external DNS.
- Disable directory listings and use split-DNS.
- Educate employees about various **social engineering tricks** and risks.
- Restrict unexpected input such as `| ; < >`.
- Avoid domain-level cross-linking for critical assets.
- Encrypt and password protect sensitive information.
- Do not enable protocols that are not required.
- Always use TCP/IP and IPSec filters.
- Configure IIS against banner grabbing.



Module Flow

So far we discussed all the necessary techniques and tools to test the security of a system or network. Now it is the time to put all those **techniques** into practice. Testing the security of a system or network using similar techniques as that of an attacker with adequate permissions is known as **penetration testing**. The penetration test should be conducted to check whether an attacker is able to reveal sensitive information in response to footprinting attempts.

	Footprinting Concepts		Footprinting Tools
	Footprinting Threats		Footprinting Countermeasures
	Footprinting Methodology		Footprinting Penetration Testing

Penetration testing is an evaluation method of system or network security. In this evaluation method, the **pen tester** acts as a malicious outsider and simulates an attack to find the security loopholes.



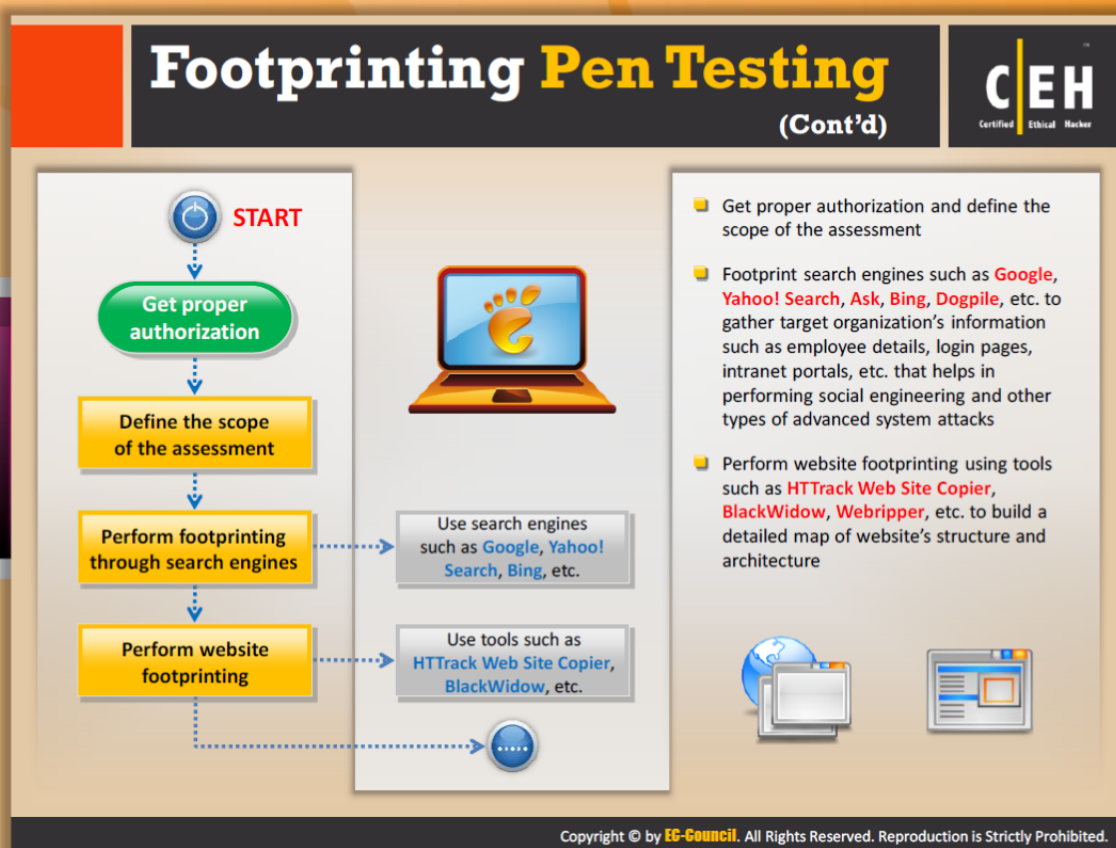
Footprinting Pen Testing

A footprinting pen test is used to determine an organization's publicly available **information on the Internet** such as network architecture, operating systems, applications, and users. In this method, the pen tester tries to gather publicly available sensitive information of the target by pretending to be an attacker. The target may be a specific host or a network.

The pen tester can perform any attack that an attacker could perform. The pen tester should try all possible ways to gather as much information as possible in order to ensure maximum scope of footprinting pen testing. If the pen tester finds any **sensitive information** on any publicly available information resource, then he or she should enter the information and the respective source in the report.

The major advantages of conducting penetration testing include:

- It gives you the chance to prevent DNS record retrieval from publically available servers.
- It helps you to avoid information leakage.
- It prevents **social engineering** attempts.



Footprinting Pen Testing (Cont'd)

Penetration testing is a procedural way of testing the security in various steps. Steps should be followed one after the other in order to ensure **maximum scope** of testing. Here are the steps involved in footprinting pen testing:

Step 1: Get proper authorization

Pen testing should be **performed** with **permission**. Therefore, the very first step in a footprinting pen test is to get proper authorization from the concerned people, such as administrators.

Step 2: Define the scope of the assessment

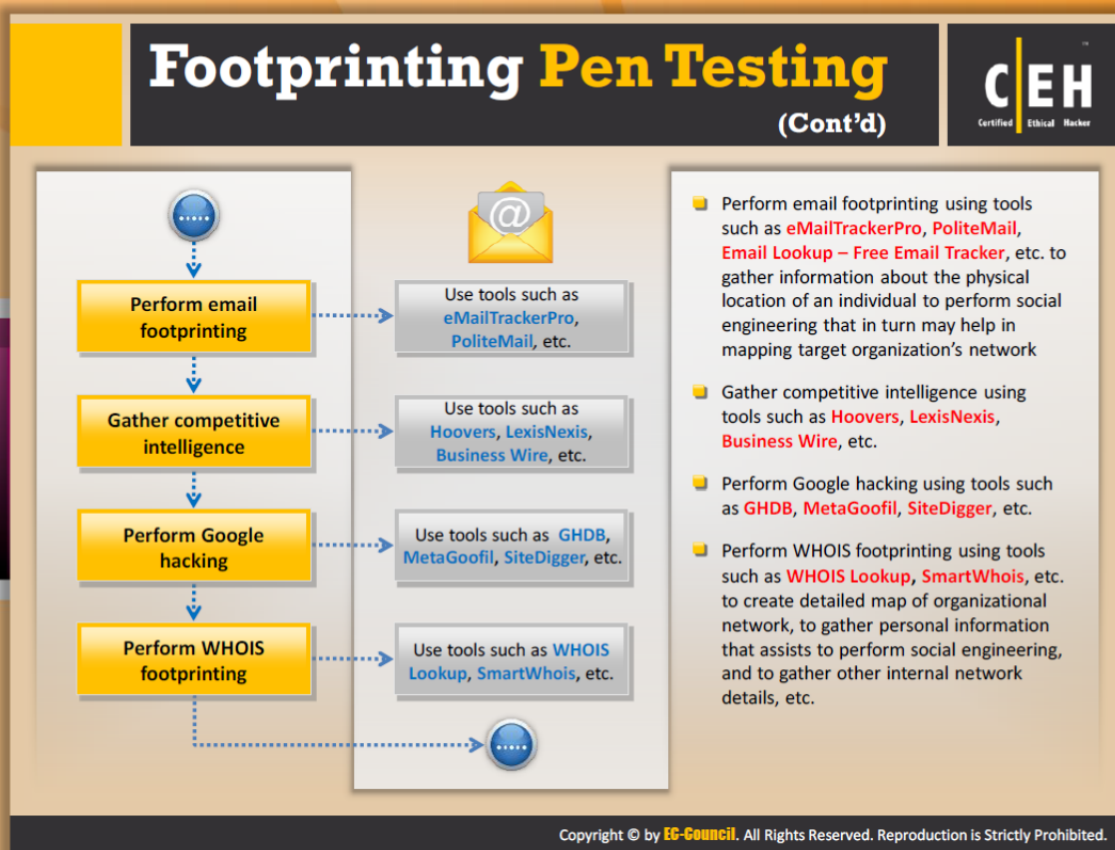
Defining the scope of the **security assessment** is the prerequisite for penetration testing. Defining the scope of assessment determines the range of systems in the network to be tested and the resources that can be used to test, etc. It also determines the pen tester's limitations. Once you define the scope, you should plan and gather sensitive information using various footprinting techniques.

Step 3: Perform **footprinting** through search engines

Footprint search engines such as Google, Yahoo! Search, Ask, Bing, Dogpile, etc. to gather the target organization's information such as employee details, login pages, intranet portals, etc. that can help in performing social engineering and other types of **advanced system attacks**.

Step 4: Perform website footprinting

Perform website footprinting using tools such as HTTrack Web Site Copier, BlackWidow, Webripper, etc. to build a detailed map of the **website's structure and architecture**.



Footprinting Pen Testing (Cont'd)

Step 5: Perform email footprinting

Perform email footprinting using tools such as eMailTrackerPro, PoliteMail, Email Lookup – Free Email Tracker, etc. to gather information about the physical location of an individual to perform **social engineering** that in turn may help in mapping the target organization's network.

Step 6: Gather competitive intelligence

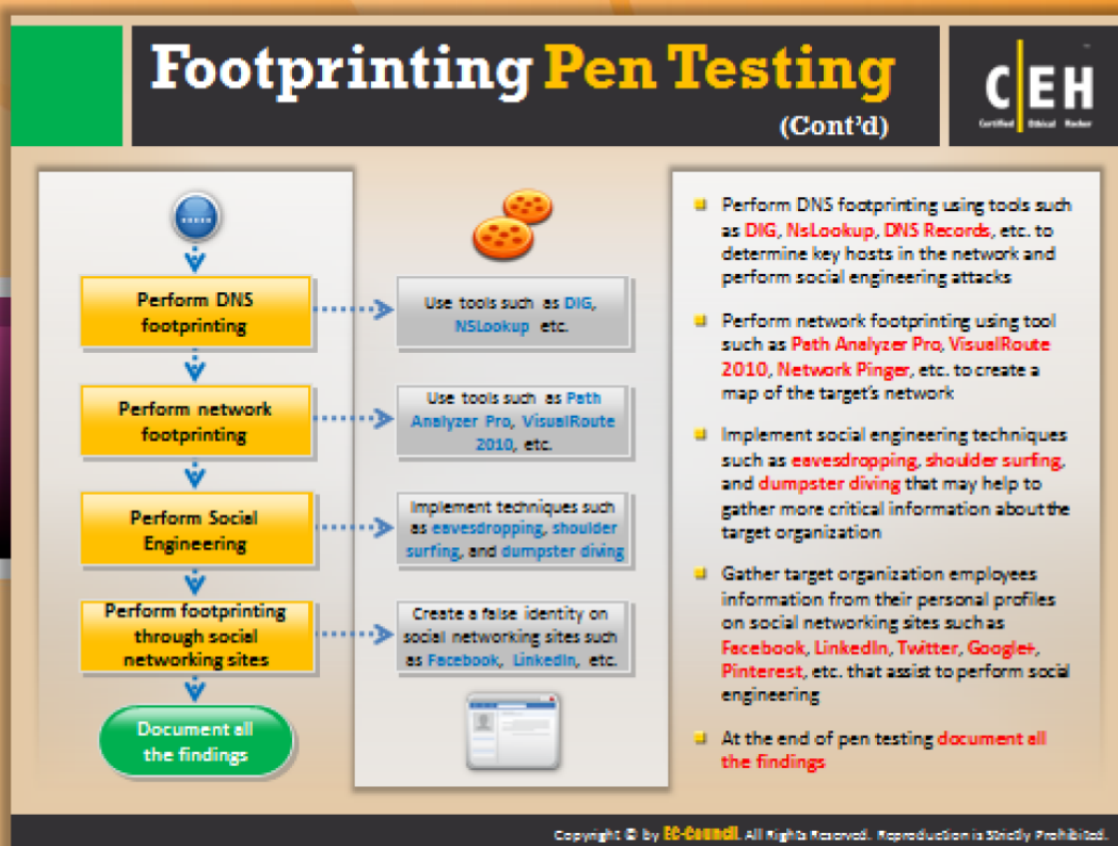
Gather competitive intelligence using tools such as **Hoovers**, SEC Info, Business Wire, etc. These tools help you to extract a competitor's information such as its establishment, location of the company, progress analysis, higher authorities, product analysis, marketing details, and much more.

Step 7: Perform Google hacking

Perform Google hacking using tools such as GHDB, MetaGoofil, SiteDigger, etc. It determines the **security loopholes** in the code and configuration of the websites. Google hacking is usually done with the help of advanced Google operators that locate specific strings of text such as versions of vulnerable web applications.

Step 8: Perform WHOIS footprinting

Perform the WHOIS **footprinting technique** to extract information about particular domains. You can get information such as domain name, IP address, domain owner name, registrant name, and their contact details including phone numbers, email IDs, etc. Tools such as SmartWhois, CountryWhois, Whois Pro, and ActiveWhois will help you to extract this information. You can use this information to perform **social engineering** to obtain more information.



Footprinting Pen Testing (Cont'd)

Step 9: Perform DNS footprinting

Perform DNS footprinting using tools such as DIG, NSlookup, DNS Records, etc. to determine key hosts in the network and perform **social engineering attacks**. Resolve the domain name to learn about its IP address, DNS records, etc.

Step 11: Perform network footprinting

Perform network footprinting using tools such as Path Analyzer Pro, VisualRoute 2010, Network Pinger, etc. to create a map of the target's network. Network footprinting allows you to reveal the network range and other **network information** of the target network. Using all this information, you can draw the network diagram of the target network.

Step 12: Perform social engineering

Implement social engineering techniques such as **eavesdropping**, **shoulder surfing**, and dumpster diving that may help to gather more critical information about the target organization. Through social engineering you can gather **target organization's** employee details, phone numbers, contact address, email address, etc. You can use this information to reveal even more information.

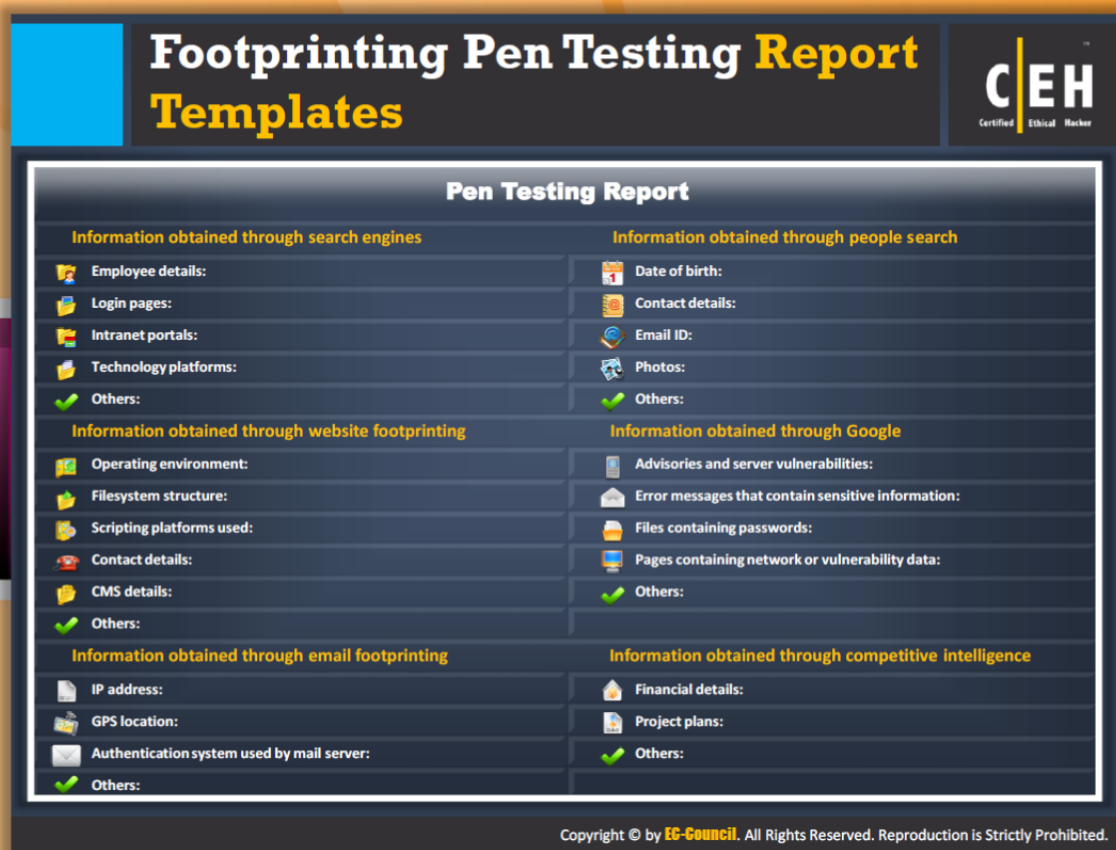
Step 13: Perform footprinting through social networking sites

Perform footprinting through social networking sites on the employees of the **target organization** obtained in footprinting through social engineering. You can gather information from their personal profiles on social networking sites such as Facebook, LinkedIn, Twitter, Google+, Pinterest, etc. that assists in **performing social engineering**. You can also use people search engines to obtain information about target person.

Step 14: Document all the findings

After implementing all the **footprinting techniques**, collect and document all the information obtained at every stage of testing. You can use this document to study, understand, and analyze the security posture of the target organization. This also enables you to find security loopholes. Once you find security loopholes, you should suggest respective countermeasures to the loopholes.

The following is a summary of footprinting **penetration testing**.



Footprinting Pen Testing Report Templates



Pen Testing Report

Penetration testing is usually conducted to enhance the **security perimeter** of an organization. As a pen tester you should gather sensitive information such as server details, the operating system, etc. of your target by conducting footprinting. Analyze the system and network defenses by breaking into its security with **adequate permissions** (i.e., ethically) without causing any damage. Find the loopholes and weaknesses in the network or system security. Now explain all the **vulnerabilities** along with respective countermeasures in a report, i.e., the pen testing report. The pen testing report is a report obtained after performing network penetration tests or security audits. It contains all the details such as types of tests performed, the **hacking techniques** used, and the results of hacking activity. In addition, the report also contains the highlights of security risks and vulnerabilities of an organization. If any vulnerability is identified during any test, the details of the cause of vulnerability along with the countermeasures are suggested. The report should always be kept **confidential**. If this information falls into the hands of attacker, he or she may use this information to launch attacks.

The pen testing report should contain the following details:



FIGURE 2.48: Pen Testing Report

Footprinting Pen Testing Report Templates (Cont'd)

CEH

Certified Ethical Hacker

Pen Testing Report

Information obtained through WHOIS footprinting Domain name details: Contact details of domain owner: Domain name servers: Netrange: When a domain has been created: Others:	Information obtained through social engineering Personal information: Financial information: Operating environment: User names and passwords: Network layout information: IP addresses and names of servers: Others:
Information obtained through DNS footprinting Location of DNS servers: Type of servers: Others:	
Information obtained through network footprinting Range of IP addresses: Subnet mask used by the target organization: OS's in use: Firewall locations: Others:	Information obtained through social networking sites Personal profiles: Work related information: News and potential partners of the target company: Educational and employment backgrounds: Others:

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Footprinting Pen Testing Report Templates (Cont'd)

Footprinting Pen Testing Report Templates (Cont'd)

CEH

Certified Ethical Hacker

Pen Testing Report

Information obtained through WHOIS footprinting Domain name details: Contact details of domain owner: Domain name servers: Netrange: When a domain has been created: Others:	Information obtained through social engineering Personal information: Financial information: Operating environment: Usernames and passwords: Network layout information: IP addresses and names of servers: Others:
Information obtained through DNS footprinting Location of DNS servers: Type of servers: Others:	
Information obtained through network footprinting Range of IP addresses: Subnet mask used by the target organization: OS's in use: Firewall locations: Others:	Information obtained through social networking sites Personal profiles: Work related information: News and potential partners of the target company: Educational and employment backgrounds: Others:

FIGURE 2.49: Pen Testing Report showing information obtained through footprinting and social engineering

Module Summary



- ❑ Footprinting is the process of collecting as much information as possible about a target network, for identifying various ways to intrude into an organization's network system
- ❑ It reduces attacker's attack area to specific range of IP address, networks, domain names, remote access, etc.
- ❑ Attackers use search engines to extract information about a target
- ❑ Information obtained from target's website enables an attacker to build a detailed map of website's structure and architecture
- ❑ Competitive intelligence is the process of identifying, gathering, analyzing, verifying, and using information about your competitors from resources such as the Internet
- ❑ DNS records provide important information about location and type of servers
- ❑ Attackers conduct traceroute to extract information about: network topology, trusted routers, and firewall locations
- ❑ Attackers gather sensitive information through social engineering on social networking websites such as Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+, etc.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

- Footprinting refers to uncovering and collecting as much information as possible about a target of attack.
- It reduces attacker's attack area to specific range of IP address, networks, domain names, remote access, etc.
- Attackers use search engines to extract information about a target.
- Information obtained from target's website enables an attacker to build a detailed map of website's structure and architecture.
- Competitive intelligence is the process of identifying, gathering, analyzing, verifying, and using information about your competitors from resources such as the Internet.
- DNS records provide important information about location and type of servers.
- Attackers conduct traceroute to extract information about: network topology, trusted routers, and firewall locations.
- Attackers gather sensitive information through social engineering on social networking websites such as Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+, etc.